Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182

Research Papers
Volume 1
Threat Assessment
RCMP/CSIS Co-operation

Commission
of Inquiry into
the Investigation
of the Bombing of
Air India Flight 182

Commission d'enquête
relative aux mesures
d'investigation prises à
la suite de l'attentat à la
bombe commis contre
le vol 182 d'Air India

The opinions expressed in these academic studies are those of the authors; they do not necessarily represent the views of the Commissioner.

Cat. No: CP32-89/5-2010E
ISBN: 978-0-660-19984-9

Available through your local bookseller or through
Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario
KIA OS5

Telephone: (613) 941-5995 or 1 800 635-7943
Fax: (613) 954-5779 or 1 800 565-7757
publications@pwgsc.gc.ca
Internet: www.publications.gc.ca

Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 Research Studies – Volume 1

Threat Assessment and RCMP/CSIS Co-operation

Table of Contents

Introduction

Kent Roach

The Commission's Research Program

Shortly after the appointment of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, a decision was made by the Commissioner, commission counsel and the research directors to commission a number of research papers on matters relevant to the Commission's broad mandate.

Research studies have long been an important part of the commission of inquiry process in Canada. For example, the McDonald Commission of Inquiry that examined activities of the Royal Canadian Mounted Police's (RCMP) activities and made recommendations that lead to the creation of the Canadian Security Intelligence Service (CSIS) in 1984 issued a number of research papers and monographs as part of its process.[1] Other commissions of inquiry at both the federal and provincial levels have followed suit with at times ambitious research agendas.[2]

Research allows commissions of inquiry to be exposed and informed by expert commentary. Research papers can be independently prepared by academics and other experts. The parties and the public are free to comment on these papers and the Commissioner is free to reject or to accept any advice provided in the research papers. The traditional disclaimer that the research paper does not necessarily represent the views of the Commission or the Commissioner is true.

The Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 faced the challenge of a particularly broad mandate that spanned the issues of the adequacy of threat assessment of terrorism both in 1985 and today, co-operation between governmental

---

1 For example, see the research studies published by the McDonald Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. J. Ll. J. Edwards *Ministerial responsibility for national security as it relates to the offices of Prime Minister, Attorney General and Solicitor General of Canada* (Ottawa: Supply and Services Canada, 1980); C.E.S. Franks Parliament and Security Matters (Ottawa: Supply and Services Canada, 1980); M.L. Friedland *National Security: The Legal Dimensions* (Ottawa: Supply and Services, 1980).

2 The Commission of Inquiry into the Activities of Canadian Officials in Relation to Maher Arar published a series of background papers. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services, 2006).

departments including the RCMP and CSIS, the adequacy of restraints on terrorism financing including funding from charities, witness protection, aviation security and terrorism prosecutions. A broad range of expertise drawn from a variety of academic disciplines was needed to address this mandate.

A commission of inquiry's research program can help create or solidify a research foundation for continued thought and policy development in the area being examined. Canadian research into terrorism related issues has generally been relatively sparse.[3] There is no dedicated governmental funding for research related to the study of terrorism and optimal counter-terrorism measures as there is in other fields such as military studies. One of my hopes is that the research program of this Commission will stimulate further investment in independent research related to terrorism and counter-terrorism.

The Commission of Inquiry was fortunate to be able to retain the majority of Canada's leading experts in many of these areas. The Commission was also able to retain a number of leading international experts to provide research of a more comparative nature. The comparative research was undertaken to determine if Canada could learn from the best practices of other democracies in many of the areas related to the mandate.

Researchers who conduct studies for a Commission of Inquiry do not have the luxury that an academic researcher normally has in conducting research and publishing their work. They must work under tight deadlines and strive to produce analysis and recommendations that are of use to the Commission of Inquiry.

A decision was made to ask our researchers to write only from public sources and indeed to write and complete papers long before the Commission's hearing process was completed. This means that the researchers may not always have had the full range of information and evidence that was available to the Commission. That said, the research papers, combined with the dossiers issued by commission counsel, provided the commissioner, the parties and the public with an efficient snapshot of the existing knowledge base.

---

3 On some of the challenges see Martin Rudner "Towards a Proactive All-of-Government Approach to Intelligence-Led Counter-Terrorism" and Wesley Wark "The Intelligence-Law Enforcement Nexus" in Vol 1 of the Research Studies.

Because of the importance of public and party participation in this Commission of Inquiry, a decision was made early on that the researchers retained by the Commission would, whenever possible, present and defend the results of their research in the Commission's hearings. A deliberate decision was made to reject the dichotomy of part one hearings focused on the past and part two processes aimed at the future. This decision reflected that much of the Commission's mandate required an examination of both the past and the future. There was also a concern that the Commissioner should be able to see the research produced for him challenged and defended in a public forum.

It is my hope that the research program will help inform the deliberations of the commission and also provide a solid academic foundation for the continued study in Canada of terrorism and the many policy instruments that are necessary to prevent and prosecute terrorism.

The Research Studies in this Volume

The research studies in the volume start with an attempt to understand both the nature of the threat of terrorism in 1985 when Air India Flight 182 was bombed killing 329 people and the contemporary threat environment. This dual orientation is required by the Commission's terms of reference which direct attention to both "the potential threat posed by Sikh terrorism before or after 1985" and "the assessment of terrorist threats in the future."[4]

This volume also contains two essays that examine the mandates and relationship between the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, two agencies that are specifically mentioned in the Commission's terms of reference. [5]Again, there is a dual focus in these studies that include both a retrospective assessment of the relation between these agencies in both the pre and post bombing periods as well as what is publicly known about their contemporary relations.

---

4 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 *Terms of Reference* b (i).

5 Ibid b (ii).

These studies also provide an introduction to both the role of terrorism financing and the relation between intelligence and evidence, important subjects that are examined in subsequent volumes of the research studies.[6]

Bruce Hoffman "Study of International Terrorism"

The Commission was fortunate to able to retain the services of Professor Bruce Hoffman of Georgetown University, one of the world's leading experts on terrorism. His wide ranging study situates the 1985 bombing of Air India Flight 182 in the context of major trends in both terrorism and counter-terrorism. Professor Hoffman notes that the bombing of Flight 182, combined with the simultaneous explosion of another bomb destined for another Air India plane in the Narita Airport, constituted the most deadly act of international terrorism until 9/11.

The first part of Professor Hoffman's paper situates the Air India bombing in light of the evolving nature of terrorism. He describes how the Air India bombing cut against the conventional wisdom of the time which was that terrorists were more interested in publicity than in killing large numbers of people. He relates the growing lethality of terrorism to the rise of religiously inspired terrorism so that by the middle of the 1990's, religiously inspired terrorist groups accounted for nearly half of all terrorist groups.

Professor Hoffman next examines the role of intelligence and law enforcement in preventing terrorism. He suggests that intelligence will play the lead role in preventing terrorism, but that this often involves a "delicate balancing act" with respect to the need to respond to the threat and the need to respect civil liberties. He points out that intelligence and police officers have different skills sets and concerns. Not all intelligence will be collected under conditions that will allow it be admitted in court. Although there are some parallels between law enforcement efforts aimed at organized crime and terrorism, Professor Hoffman warns that terrorism is an unique crime because it is intended to have effects beyond the act and the immediate victims.

---

6 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 *Terrorism Financing and Charities* Vol 2 of the Research Studies; Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 *The Relationship Between Intelligence and Evidence* Vol. 4 of the Research Studies.

Professor Hoffman concludes his study with a survey of a variety of practices in the financing of terrorism. He stresses how suicide bombing can produce great human and financial costs with only modest investments. He concludes with a series of recommendations about the importance of both domestic and foreign intelligence in preventing terrorist acts, whether the 1985 bombing of Air India Flight 182 or some future terrorist attack.

Michael A. Hennessy "A Brief on International Terrorism"

Professor Michael Hennessy, the Chair of the Department of History at the Royal Military College of Canada, provides an historical overview of terrorism, noting that the term was first popularized by Edmund Burke as a pejorative term against French revolutionaries. He examines the multiplicity of causes and approaches to terrorism including some acts of terrorism that can be seen as an instrumental and rational tactic while others may be related to a desire for publicity or simply an expression of "groupthink" by a small number of individuals.

Professor Hennessy concludes that the Air India bombing could have been formulated instrumentally as retaliation against the Indian government, but that it could also have been an act to build cohesion and identity among a small group of individuals. His essay reminds us of the complexity of terrorism and its many different motivations.

Peter M. Archambault "Context is Everything: The Air India Bombing, 9/11 and the Limits of Analogy"

Dr. Peter Archambault who has served as a Research Director both for this Commission and for the Minister's Monitoring Committee on Change within the Department of National Defence and as an adjunct associate professor at the Royal Military College of Canada, critically examines the idea that the Air India bombing was Canada's 9/11 or the result of an intelligence failure.

Dr. Archambault warns that no intelligence agency is omniscient and that blaming terrorist attacks on intelligence failures may shift responsibility for terrorist attacks away from the terrorist themselves and discount the

often unknown successes of intelligence. He also argues that the Air India bombing likely fits better on the criminal end of a spectrum of threats to Canada whereas the threat of Al Qaeda is much closer to the war end of the spectrum. He argues that a criminal justice system response to Al Qaeda terrorism will not be sufficient.

Martin Rudner "Towards a Proactive All-of-Government Approach to Intelligence-Led Counter-Terrorism"

The next essay in this volume is authored by Martin Rudner, a Distinguished Research Professor Emeritus at the Norman Paterson School of International Affairs at Carleton University. He outlines a cycle of terrorism. The steps of the cycle are 1) strategic planning 2) recruitment of activists and operatives 3) training 4) communications 5) resourcing 6) financing including fund-raising and money transfers 7) procurement, preparation and delivery of materiel 8) creating an infrastructure for sleeper cells 9) propaganda and incitement 10) terrorist penetration into sensitive parts of government 11) tactical preparations and reconnaissance on targets and finally 12) terrorist assaults. Professor Rudner argues that each step of this cycle provides its own opportunities for counter-terrorism measures including the use of various human, technical and signals intelligence as well as the sharing of intelligence.

Professor Rudner proposes greater co-ordination of intelligence efforts by moving the Integrated Threat Assessment Centre (ITAC) created in 2004 into the Privy Council Office and having ITAC report to an enhanced office of the National Security Advisor to the Prime Minister. He proposes that the National Security Advisor should be able to dispense additional budgetary and personnel resources to operational agencies to allow them to focus more attention on particular counter-terrorism targets and objectives. These objectives would be informed by intelligence so that intelligence analysis would drive intelligence collection. The approach that he proposes can be contrasted with the traditional approach in which intelligence analysis follows intelligence collection. Professor Rudner also warns that more effective intelligence analysis will require increased education in the universities as well as attractive career paths in government.

Wesley Wark "The Intelligence-Law Enforcement Nexus"

Professor Wesley Wark of the Department of History and the Munk Centre at the University of Toronto provides an historical overview of relationships between CSIS and the RCMP as seen through the prism of the relation between law enforcement and intelligence. He stresses the limits faced by researchers working only with public documents including the inevitable reliance on judgments made by the Security Intelligence Review Committee, the body that has most frequently evaluated the relationship between the RCMP and CSIS.

Professor Wark suggests that the greatest energy in the early years of CSIS was devoted to the civilization project with both the 1987 report of the Independent Advisory Team and the five year Parliamentary review not directly examining the CSIS/RCMP relationship. To this extent, a conscious decision was made to separate CSIS and the RCMP. The 1992 SIRC report on the Air India investigation, as well as reports by SIRC in 1998 and 1999, revealed some tension between CSIS and the RCMP mainly stemming from their different mandates and CSIS's concern about disclosing sources and methods. Early memoranda of understandings and directives conceived of the relation between CSIS and the RCMP being based on a one-way flow of intelligence from CSIS to the RCMP with only some changes being made post 9/11 through the creation of joint management teams, the Integrated Threat Assessment Centre and recognition of the need for the RCMP to generate intelligence to inform its investigative function.

Professor Wark also examines the public record about Air India as an example of an intelligence failure. Failures to translate and retain wiretaps on Talwinder Singh Parmar and to conduct adequate surveillance are in his view clear indications of a failure of intelligence collection. He also finds evidence of intelligence failure with respect to the analysis of the specificity of the threat from Sikh terrorism while also warning that intelligence failures may be widespread.

Jean-Paul Brodeur "The Royal Canadian Mounted Police and the Canadian Security Intelligence Service: A Comparison Between Occupational and Organizational Cultures"

Professor Jean-Paul Brodeur, the Director of the International Centre of Comparative Criminology Centre at the University of Montreal, provides a wide ranging comparison of the organizational and occupational cultures of the RCMP and CSIS. Like Professor Wark he stresses the limits of working with public documents especially the public reports of SIRC. He stresses that CSIS as originally created in 1984 inherited most of its personnel and working assumptions from the former Security Service of the RCMP. The emphasis was more on short-term tactical analysis and case based operations than strategic intelligence. Based on his own research into detective work, Professor Brodeur also suggests that the failure to make arrests in the early stages of the bombing investigation was likely critical and more likely stemmed from transition issues and competition between the two agencies than any differences between the professional cultures of police and security intelligence agencies.

Professor Brodeur locates much of the competition and tension between CSIS and the RCMP in the relation between intelligence and evidence and the concerns of CSIS to protect their files, surveillance records, employees and human sources from disclosure in court. He focuses on human sources and informers as the most difficult area, noting that most good informers will play an active role. He suggests that security intelligence agencies need to become familiar with some of the techniques of witness protection used by the police, but also that disclosure requirements in criminal prosecutions should be clarified.

Professor Brodeur concludes by examining a number of points of contrast between the RCMP and CSIS including the former organization's orientation towards evidence and the courts and the latter's orientation towards secret intelligence and the executive. He suggests that these differences between the two organizations may require the RCMP to target the same individual or group as CSIS, but for its own evidentiary purposes. Such a process would be supervised by a senior level co-ordination committee.

Conclusion

The six essays in this volume taken together provide an introduction to the threat environment and the evolving nature of terrorism as well as an introduction to the different mandates of CSIS and the RCMP in responding to this threat environment. The essays also contain a number of interesting recommendations for possible reforms including the enhancement of the co-ordination function of the National Security Advisor within the Privy Council Office, greater co-ordination between the targeting decisions of CSIS and the RCMP and the use of witness protection programs by security intelligence agencies. The first essay in this volume also provides an introduction to the topic of terrorism financing that will be examined in volume 2 of the research studies. The last two essays in this volume also introduce the theme of the relationship between secret intelligence and public evidence that will be examined in greater detail in volume 4 of the research studies.

Study of International Terrorism
Written Expert Report Submitted to
The Commission of Inquiry Into the Investigation of the Bombing of Air India 182

Professor Bruce Hoffman
Georgetown University, Washington, D.C.

Before 9/11, there was Air India Flight 182. In the entirety of the 20th Century no more than 14 terrorist incidents——international and domestic[1]——had killed more than 100 persons.[2] Of these, the 1985 mid-air bombing of Air India flight 182 held the nefarious distinction of being the most deadly act of *international* terrorism in history.[3] Only the death and destruction wrought on September 11th 2001 by the four hijacked aircraft, the loss of the passengers on each of those flights coupled with the death toll on the ground at the World Trade Center and the Pentagon eclipsed the Air India bombing in terrorist lethality.

Significantly, too, from a purely terrorist operational perspective, spectacular or significant *simultaneous* acts of terrorism——like the inflight Air India 182 bombing and the explosion less than an hour earlier as baggage was being transferred at Tokyo's Narita Airport from Canadian Pacific Flight 003 (recently arrived from Vancouver, Canada) to a waiting Air India flight (two airport workers were killed and four others wounded)[4]——are relatively uncommon. For reasons still not well understood, terrorists historically have rarely contemplated and typically have not been able to execute coordinated operations. This was doubtless less of a choice than a reflection of the logistical and other organizational hurdles and constraints that all but the most determined or sophisticated terrorist groups were unable to overcome. Indeed, this was one reason why the world was so galvanized by the synchronized attacks on September 11th 2001. The orchestration of that operation, coupled with its unusually high death and casualty tolls, stood out in a way that no previous terrorist operation had. In the three decades that preceded 9/11 there were comparatively few successfully executed, simultaneous terrorist spectaculars.[5] The mid-air bombing of Air India Flight 182 and the Narita Airport explosion were thus

---

1 International terrorism is defined as incidents in which the perpetrators go abroad to strike their targets, select victims or targets associated with a foreign state, or create an international incident by attacking airline passengers or equipment. Domestic terrorism is defined as incidents perpetrated by local nationals against a purely domestic target. See "Terrorism Update: Understanding the Terrorism Database" in Oklahoma City National Memorial Institute for the Prevention of Terrorism, *MIPT Quarterly Bulletin*, First Quarter 2002, p. 4.

2 Brian M. Jenkins, "The Organization Men: Anatomy of a Terrorist Attack," in James F. Hoge, Jr. and Gideon Rose, *How Did This Happen? Terrorism and the New War* (NY: Public Affairs, 2001), p.5.

3 The domestic terrorist incident responsible for the largest number of deaths was the fire deliberately set by terrorists at a movie theater in Abadan, Iran in 1979 that claimed the lives of 477 persons. See Richard Falkenrath, Robert D. Newman, and Bradley A. Thayer, *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack* (Cambridge, MA: MIT Press 1998), "Table 1. Mass-casualty Attacks By Terrorists in the Twentieth Century (100 or more fatalities), p. 47.

4 See Stewart Beli, *Cold Terror: How Canada Nurtures and Exports Terrorism Around The World* (Toronto: John Wiley & Sons Canada, Ltd., 2007), p. 37.

5 See Jenkins, "The Organization Men: Anatomy of a Terrorist Attack" supra

also distinctive for their attempted coordinated destruction of two Air India passenger aircraft while in flight.[6]

This report, however, is not specifically about the 1985 Air India Flight 182 and Narita Airport bombings. There are others, more qualified and more expert to assess and analyze all the dimensions of that terrorist operation and its aftermath. Rather, this report seeks to situate these two incidents within the context of our understanding and knowledge of terrorism both at the time of the bombings and today. And, by doing so, to assess the impact and meaning of the 1985 bombings within the broader pattern of international terrorism both in 1985 and as it has unfolded since.

The report is divided into three sections. The first section addresses what terrorism was like and how it was perceived in the middle of the 1980s and how terrorism has changed and evolved since. Within this context, it also examines how Sikh extremism fits into the paradigm of religiously inspired terrorism; how terrorism was then structured and what its "place" was in the world of 1985 compared with today. The second section addresses terrorism, law enforcement and intelligence. The issues it considers include: the role of terrorism and law enforcement in today's climate; the interplay between intelligence and evidence (e.g., evidence gathering compared with intelligence gathering); whether intelligence has become the primary instrument in countering terrorists as opposed to law enforcement and conviction of criminals; the goals of and proper tools along the continuum of law enforcement and counterterrorism; and, the characteristics of terrorism both as we encounter them today and in historical perspective that makes the issue of witness protection and the use of informers within radical communities necessary. The third, and final, section focuses on terrorism financing issues. It seeks to assess what aspects of terrorist financing today remain the same or have changed from the 1980s; the goal of government interdiction of terrorist financing; and, what terrorists typically spend their money on.

---

6 Apart from the attacks on the same morning in October 1983 of the U.S. Marine barracks in Beirut (241 persons were killed) and a nearby French paratroop headquarters (where 60 soldiers perished) and the series of attacks that occurred in Bombay in March 1993, where a dozen or so simultaneous car bombings rocked the city, killing nearly 300 persons and wounding more than 700 others no other simultaneous terrorism incidents in the 20th Century claimed more than 100 lives. The other incidents, with lower levels of lethality, include: the 1981 hijacking of three Venezuelan passenger jets by a mixed commando of Salvadoran leftists and Puerto Rican *independistas*; the attacks on the Rome and Vienna airports staged by the Abu Nidal Group in December 1986, where 20 persons were killed; the IRA's near simultaneous assassination of Lord Mountbatten and the remote-control mine attack on British troops in Warrenpoint, Northern Ireland in 1979 that claimed the lives of 18 soldiers. Also the dramatic 1970 hijacking of four commercial aircraft by the PFLP (Popular Front for the Liberation of Palestine), two of which were brought to and then dramatically blown up at Dawson's Field in Jordan, there have been comparatively few successfully executed, simultaneous terrorist spectaculars.

Terrorism Then (1985) And Now (2007): Context and Perspectives

For more than two decades the seminal compendium of annual international terrorism incidents and analysis arguably has been the U.S. Department of State's *Patterns of Global Terrorism*. This report, published annually every April by the State Department since 1985 in accordance with requirements stipulated by the U.S. Congress, reviews the previous years' trends in international terrorism, highlights and discusses particularly significant terrorist incidents and provides a detailed region-by-region survey of the most important developments in terrorism that have affected individual countries. It is therefore worthwhile to quote verbatim and in its entirety the first paragraph of the 1985 report, which began with a terse, retrospective summary of "The Year in Review":

> International terrorists had a banner year in 1985. They carried out more attacks than in any year since the decade began; caused more casualties——**especially fatalities over that same period (329 alone occurred when an Air India jetliner was blown up in June)**; [my emphasis] conducted a host of spectacular, publicity-grabbing events that ultimately ended in coldblooded murder; increasingly turned to business and more accessible public targets as security at official and military installations was strengthened against terrorism and, in so doing, counted among their victims a record number of innocent bystanders; and finally, gave pause to international travelers worldwide who feared the increasingly indiscriminate nature of international terrorism.[7]

Thus, in what was being cited as a banner year in the already sufficiently egregious annals of international terrorism, it is noteworthy that the one incident singled out for specific attention——exemplifying the heinous loss of life, targeting of an indisputably "soft" target, and that had profound psychological repercussions on attitudes towards air travel, was the Air India bombings.

---

7 United States Department of State, *Patterns of Global Terrorism 1985* (Washington, D.C.: U.S. Department of State, April 1985), p. 1.

That the Air India explosions should have generated as much shock, revulsion, and surprise as they did was because the death toll from the two bombings cut so much against the grain of contemporary thinking about terrorism at that time. The conventional wisdom in 1985——as it had been for at least a decade before and would endure for nearly two more——was that terrorists were more interested in publicity than in killing. Even though terrorists had the capability to inflict large numbers of casualties with bombs in public areas, the contemporary reasoning went, that they rarely did so or——perhaps more tellingly——even attempted to do so.[8] It was thus deduced that terrorists likely acted under self-imposed restraints. Mass, indiscriminate murder, terrorists were thought to have reasoned, would alienate the very audience they wished to recruit or at least influence. Not only would such wanton acts of violence alienate their perceived or actual constituents, terrorism experts maintained, but it would also undermine their claims of legitimacy and recognition from the international community who they hoped to impress, intimidate, and influence through often spectacular and dramatic——albeit tightly controlled and well-orchestrated——acts of violence. Moreover, terrorists——many observers at the time concluded, were able to achieve publicity and other objectives through relatively discrete acts of violence, without needing to inflict widespread casualties.[9]

This pattern had been observed consistently in the activities of both types of terrorist organizations that predominated in the mid-1980s: left-wing ideological groups[10] and ethno-nationalist/separatist organizations.[11] Both these terrorist entities appeared to be cognizant of the likelihood that acts of mass destruction or bloodshed would result in public revulsion, alienating potential supporters and gaining the sympathy of the international community as well as triggering severe government measures. Their overriding tactical imperative, accordingly, was to tailor

---

8 See, for example, the arguments presented in Walter Laqueur, "Postmodern Terrorism," *Foreign Affairs*, vol. 75, no. 5 (September-October 1996), pp. 24-36; and, Ehud Sprinzak, "The Great Superterrorism Scare," *Foreign Policy*, no. 112 (Fall 1998), pp. 110-125.

9 See, for instance, J. Bowyer Bell, *A Time of Terror: How Democratic Societies Respond to Revolutionary Violence* (New York: Basic Books, 1978), p. 121.Walter Laqueur, *Terrorism* (London: Weidenfeld and Nicolson, 1977), p. 231; Jeffrey D. Simon, *Terrorists and the Potential Use of Biological Weapons: A Discussion of Possibilities* (Santa Monica, CA: RAND, R-3771-AFMIC, December 1989), p. 12.

10 Movements with a Marxist-Leninist, Maoist, Trotsky-ist or some combination thereof in orientation.

11 For example, such as the various constituent group members of the Palestine Liberation Organization (e.g., al-Fatah, the Popular Front for the Liberation of Palestine, al-Sa'iqa); the Provisional Irish Republican Army; the Basque group, ETA; the Puerto Rican *independista* movement in the United States and the FLQ in Canada.

deliberately their violent acts to appeal to their constituents. As part of this calibration, though, they also sought to use their violence to impress, intimidate, coerce, or otherwise embarrass the principle object of their violence——most often, the ruling government or regime the terrorists were fighting against.

These terrorist groups thus engaged in highly selective and mostly discriminate acts of violence. They chose for bombing various symbolic targets representing the source of their animus (i.e., embassies, banks, national airline carriers, etc.) or kidnapped and assassinated specific persons whom they blamed for economic exploitation or political repression in order to attract attention to themselves and their causes. In this respect, these terrorists' violence was calibrated in such a manner as to appeal to their actual or perceived constituents and thus was kept within the bounds of what the terrorists believed their constituency deemed "acceptable." These groups were thus seen as being careful not to undertake actions that might alienate their supporters and sympathizers. They appeared to be cognizant of the likelihood that acts of mass destruction or bloodshed might result not only in public revulsion and alienation but, equally as important, that it might trigger severe governmental reprisals or countermeasures as well. Further, it also risked creating a crisis that governments could seize upon to justify severe repressive measures to eliminate completely any organization that dared to employ such heinous weapons.

For this reason, the violence used by left-wing terrorists, for example, was always narrowly proscribed. Their self-styled crusade for social justice therefore was often typically directed against governmental or commercial institutions or persons whom they believed represented capitalist exploitation or political repression and a fundamentally corrupt and inequitable "system." Specific individuals——wealthy industrialists such as Hanns Martin Schleyer, who was kidnapped and murdered by the German Red Army Faction (RAF) in 1977, or distinguished parliamentarians like Aldo Moro, who the Italian Red Brigades similarly abducted and executed the following year, alongside parliamentarians, mayors, councilors, lower-ranking government officials, ordinary civil servants, factory managers, union leaders, etc.——were most often targeted. When the left did resort to bombing, the violence was conceived in equally "symbolic" terms. In this sense, although the damage and destruction that often resulted were certainly not symbolic, the act itself was meant to dramatize or call attention to the terrorists' grievances or political cause and often specifically not to kill anyone.

This approach was not entirely dissimilar from that taken by the more prominent ethno-nationalist and separatist groups of that era: the constituent member groups of the Palestine Liberation Organization, the Provisional Irish Republican Army (PIRA), and the Basque separatist group ETA, among them. Although acts of terrorism committed by this category were frequently more destructive and caused more casualties than those of their left-wing counterparts, the same self-imposed constraints and balancing act of finding a level of violence acceptable to their actual or perceived constituents, seemed evident. In a broader sense, ethno-nationalist and separatist terrorism was also designed to appeal to international as well as internal opinion in support of the terrorists' irredentist or nationalist aims. Hence, to continue to receive the support of their constituency, generate sympathy among the international community and, perhaps also forestall massive governmental countermeasures, these terrorists also strove to regulate and calibrate their violence. The vast majority of their targets, accordingly, were often individuals: confined to low-ranking government officials, ordinary soldiers or policemen, other so-called "agents of the state," and members of rival communities or ethnic groups.

In addition, however radical or revolutionary any of these groups may have been politically, the vast majority of them were fundamentally conservative in their operations. Terrorists at the time were said to be demonstrably more "imitative than innovative": having a very limited tactical repertoire that was mostly directed against a similarly narrow target set.[12] They were judged as hesitant to take advantage of new situations, let alone to create new opportunities. Accordingly, what little innovation that was observed was more in the terrorists' choice of targets[13] or in the methods used to conceal and detonate explosive devices than in any particularly innovative tactics.

Indeed, there was general acceptance of the observation made famous by the RAND Corporation's Brian Michael Jenkins, one of the leading terrorism analysts both then and now, that "Terrorists want a lot of people watching and a lot of people listening and not a lot of people dead."[14] This maxim was applied directly to any potential significant increase in terrorism's lethality and in turn was often used to explain the paucity of actual known

---

12 Brian Michael Jenkins, *International Terrorism: The Other World War* (Santa Monica, CA: The RAND Corporation, R-3302-AF, November 1985), p. 12.

13 For example, the 1985 hijacking of the Italian cruise ship, the *Achille Lauro*, by Palestinian terrorists as opposed to the more typical terrorist hijacking of passenger aircraft.

14 Brian Michael Jenkins, "International Terrorism: A New Mode of Conflict" in David Carlton and Carlo Schaerf (eds.), *International Terrorism and World Security* (London: Croom Helm, 1975), p. 15.

plots, much less verifiable incidents involving terrorist attempts to kill en masse. Accordingly, it was reasoned, terrorists would continue to keep their violence within certain amorphous, but nonetheless perceived self-imposed bounds. Because, it was also argued, terrorists were fundamentally rational,[15] they would not risk alienating the international community, whose acceptance, legitimization and recognition, they craved by acts of widespread carnage.[16]

Despite the events of the first half of the 1980s——when a series of high-profile and particularly lethal suicide car and truck-bombings directed against American diplomatic and military targets in the Middle East (in one instance resulting in the deaths of 241 Marines)——many analysts saw no need to revise these arguments. In 1985, Jenkins, for example, again reiterated that, "simply killing a lot of people has seldom been one terrorist objective . . . Terrorists operate on the principle of the minimum force necessary. They find it unnecessary to kill many, as long as killing a few suffices for their purposes."[17]

Thus, the conventional wisdom on terrorism held that violence was employed less as a means of wrecking death and destruction than as a way to appeal to and attract supporters, focus attention on the terrorists and their causes or to attain a tangible political aim or concession——for example, the release of imprisoned brethren, some measure of political autonomy, independence for an historical homeland or a change of government. Terrorists therefore believed that only if their violence were calculated or regulated would they be able to obtain the popular support or international recognition they craved or attain the political ends they desired. Indeed, as one PIRA fighter from this era of terrorism once explained, "You don't just bloody well kill people for the sake of killing them."[18]

However, throughout the early- to mid-1980s these self-imposed constraints were clearly eroding. Terrorist attacks were undeniably

---

15 See, for example, the studies conducted by The RAND Corporation during the 1970s for Sandia National Laboratories and in particular, Gail Bass, Brian Jenkins, et. al, *Motivations and Possible Actions of Potential Criminal Adversaries of U.S. Nuclear Programs* (Santa Monica, CA: The RAND Corporation, R-2554-SL, February 1980).

16 See, for example, the discussion in Peter deLeon, Bruce Hoffman, Brian Jenkins, and Konrad Kellen, *The Threat of Nuclear Terrorism: A Reexamination* (Santa Monica, CA: The RAND Corporation, N-2706, January 1988), pp. 4-6.

17 Brian Michael Jenkins, *The Likelihood of Nuclear Terrorism* (Santa Monica, CA: The RAND Corporation, P-7119, July 1985), p. 6.

18 Quoted in Gerald McKnight, *The Mind of the Terrorist* (London: Michael Joseph, 1974), p. 179.

becoming increasingly more lethal and more homicidal intentions were starting to become more evident. Attacks——such as the 1983 and 1984 suicide bombings of the American embassies in Beirut, the 1983 suicide attack on the U.S. Marine Corps barracks at Beirut International Airport, and the Air India Flight 182 bombing——did not neatly conform to the tactical stereotype of terrorism in previous years. Among the reasons for terrorism's growing lethality at this time may simply have been that at least some terrorists concluded that attention——public, governmental and media——was no longer as readily obtained as it once was. To the terrorists' mind perhaps, these three pivotal audiences had become increasingly inured or de-sensitized to the continuing litany of terrorist incidents or by the repeated occurrence of non- or less-lethal operations, such as airline hijackings, assassinations of targeted individuals, or low-level though indiscriminate bombings, whose death tolls were counted in the single digits or tens and rarely, if ever, in the scores, much less hundreds. Accordingly, it was reasoned terrorists felt themselves pushed to undertake ever more dramatic or destructively lethal deeds in order to achieve the same effect that a less ambitious or bloody action may have had in the past. The same argument is relevant today, too. The clearest explication of this mindset was offered in 1995 when Timothy McVeigh, the convicted bomber of the Alfred P. Murrah Federal Building in Oklahoma City, was asked by his attorney whether he could not have achieved the same effect of drawing attention to his grievances against the U.S. government without killing anyone, he reportedly replied: "That would not have gotten the point across. We needed a body count to make our point."[19] In this respect, McVeigh may have felt driven to surpass in terms of death and destruction previous attacks by terrorists in order to guarantee that his attack would also be assured the requisite media coverage and public and governmental attention. This equation by the terrorists themselves of publicity and carnage with attention and success may thus have had the effect of locking some terrorists into an unrelenting upward spiral of violence in order to retain the media and public's interest.[20] Ramzi Ahmad Yousef, the convicted mastermind of the 1993 New York World Trade Center bombing, for instance, reportedly planned to follow that incident with the simultaneous in-flight bombings of 11 U.S. passenger airliners.[21]

---

19 Quoted in James Brooke, "Newspaper Says McVeigh Described Role in Bombing," *New York Times*, 1 March 1997.

20 See, for example, David Hearst, "Publicity key element of strategy," *The Guardian* (London), 31 July 1990; and, David Pallister, "Provos seek to 'play havoc with British nerves and lifestyle'," *The Guardian* (London), 31 July 1990.

21 James Bone and Alan Road, "Terror By Degree," *The Times Magazine* (London), 18 October 1997

Second, in some cases, revenge and retaliation for both actual and perceived wrongs inflicted by a hated government, rival ethnic group or predatory majority population may also have played a salient role in terrorist motivations and changes in operational intentions at this time. For example, one of the more sanguinary terrorist incidents of the time——the brutal machine-gun and hand-grenade attack on a Jewish synagogue in Istanbul in September 1986, that claimed the lives of 22 worshippers——was justified by its perpetrator, the Abu Nidal Organization, as revenge for a recent Israeli raid on a Palestinian guerrilla base in southern Lebanon.[22]

And, finally, the rise of terrorism motivated by religious imperatives during the first half of the 1980s played a singularly critical role in terrorism's increasing lethality at this time. The connection between religion and terrorism of course was not new.[23] However, while religion and terrorism share a long history, until the 1980s, this variant was mostly overshadowed by the ideologically-motivated (e.g., left-wing) and ethno-nationalist or separatist terrorism previously discussed. Indeed, none of the 11 identifiable terrorist groups[24] active in 1968 (the year credited with marking the advent of modern, international terrorism) could be classified as religious.[25] Not until 1980 in fact——as a result of repercussions from the revolution in Iran the year before——do the first "modern" religious terrorist groups appear:[26] but they amount to only two of the 64 groups active that year. Twelve years later, however, the number of religious terrorist groups had increased nearly six-fold, representing a quarter (11 of 48) of the terrorist organizations that carried out attacks in 1992. By 1994, a third (16) of the 49 identifiable terrorist groups could be classified as religious in character and/or motivation, and by the middle of the 1990s they accounted for nearly half (26 or 46 percent) of the 56 known terrorist groups active that year.[27]

---

22 Karen Gardela and Bruce Hoffman, *The RAND Chronology of International Terrorism for 1986* (Santa Monica, CA: RAND Corporation, R3890-RC, March 1990), p. 54.

23 As David C. Rapoport points out in his seminal study of what he terms "holy terror," until the nineteenth century, "religion provided the only acceptable justifications for terror" (see David C. Rapoport, "Fear and Trembling: Terrorism in Three Religious Traditions," *American Political Science Review*, Vol. 78, No. 3, September 1984, p. 659).

24 Numbers of active, *identifiable* terrorist groups from 1968 to the present are derived from The RAND Corporation Terrorism Databases.

25 Admittedly, many contemporary terrorist groups——such as the overwhelmingly Catholic Provisional Irish Republic Army; their Protestant counterparts arrayed in various Loyalist paramilitary groups like the Ulster Freedom Fighters, the Ulster Volunteer Force, and the Red Hand Commandos; and the predominantly Muslim Palestine Liberation Organization——all have a strong religious component by virtue of their membership. However, it is the political and not the religious aspect that is the dominant characteristic of these groups, as evidenced by the pre-eminence of their nationalist and/or irredentist aims.

26 The Iranian-backed Shi'a groups al-Dawa and the Committee for Safeguarding the Islamic Revolution.

27 Data derived from the RAND Terrorism Databases.

The implications of terrorism motivated by a religious imperative for higher levels of lethality is further borne out by the time series investigation conducted by two American economists in the late 1990s. Using quantitative methodology they came to the conclusion that the "growth of religious terrorism appears to be behind the increased severity of terrorist attacks witnessed over the previous decade.[28] This causal relationship between religion and higher lethality may also be seen in the violent record of various Shi'a Islamic groups during the 1980s. Although these organizations committed only eight percent of all recorded international terrorist incidents between 1982 and 1989, they were nonetheless responsible for nearly 30 percent of the total number of deaths during that time period.[29]

Indeed, some of the most significant——and bloody——terrorist acts of 1990s all had some religious element present. They included:

- the 1993 bombing of New York City's World Trade Center by Islamic radicals who deliberately attempted to topple one of the twin towers onto the other;

- the series of 13 near-simultaneous car and truck bombings that shook Bombay, India in February 1993, killing 400 persons and injuring more than 1,000 others, in reprisal for the destruction of an Islamic shrine in that country;

- the December 1994 hijacking of an Air France passenger jet by Islamic terrorists belonging to the Algerian Armed Islamic Group (GIA) and the attendant foiled plot to blow up themselves, the aircraft and the 283 passengers on board precisely when the plane was over Paris, thus causing the flaming wreckage to plunge into the crowded city below;[30]

---

28 Walter Enders and Todd Sandler, "Is Transnational Terrorism Becoming More Threatening? A Time Series Investigation," Unpublished ms. (October 1998), Abstract before p. 1 and p. 21.

29 Between 1982 and 1989 Shi'a terrorist groups committed 247 terrorist incidents but were responsible for 1057 deaths. Source: The RAND Corporation Terrorism Databases.

30 The hijackers' plans were foiled, however, after the French authorities learned of their intentions and ordered commandos to storm the aircraft after it had landed for re-fuelling in Marseilles.

- the March 1995 sarin nerve gas attack on the Tokyo subway system, perpetrated by an apocalyptic Japanese religious cult (Aum Shrinrikyo) that killed a dozen persons and wounded more than 5,000 others and reports that the group also planned to carry out identical attacks in the U.S.;[31]

- the bombing of an Oklahoma City federal office building in April 1995, where 168 persons perished, by two Christian Patriots seeking to foment a nation-wide race revolution;[32]

- the wave of bombings unleashed in France by the Algerian Armed Islamic Group (GIA) between July and October 1995, of metro trains, outdoor markets, cafes, schools and popular tourist spots, that killed eight persons and wounded more than 180 others;

- the assassination in November 1995 of Israeli Prime Minister Itzhak Rabin by a religious Jewish extremist and its attendant significance as the purported first step in a campaign of mass murder designed to disrupt the peace process;

- the Hamas suicide bombers who turned the tide of Israel's national elections with a string of bloody attacks that killed 60 persons between February and March 1996;

- the Egyptian Islamic militants who carried out a brutal machine-gun and hand grenade attack on a group of Western tourists outside their Cairo hotel in April 1996 that killed 18;

- the June 1996 truck bombing of a U.S. Air Force barracks in Dhahran, Saudi Arabia, by religious militants opposed to the reigning al-Saud regime where 19 persons perished

---

31 Nicholas D. Kristof, "Japanese Cult Planned U.S. Attack," *International Herald Tribune* (Paris), 24 March 1997; and, Robert Whymant, "Cult planned gas raids on America," *The Times* (London), 29 March 1997.

32 It is a mistake to view either the American militia movement and other contemporary white supremacist organizations (from which McVeigh and his accomplice Terry L. Nichols emerged) as simply militant anti-federalist or extremist tax-resistance movements. The aims and motivations of these groups in fact span a broad spectrum of anti-federalist and seditious beliefs coupled with religious hatred and racial intolerance, masked by a transparent veneer of religious precepts. They are bound together by the ethos of the broader Christian Patriot movement which actively incorporates Christian scripture in support of their violent activities and uses biblical liturgy to justify their paranoid call-to-arms. For a more detailed analysis, see Bruce Hoffman, *Inside Terrorism* (London: Victor Gollancz and New York: Columbia University Press, 1998), pp. 105-120.

- the unrelenting bloodletting by Islamic extremists in Algeria itself that has claimed the lives of more than an estimated 75,000 persons there since 1992;

- the massacre in November 1997 of 58 foreign tourists and four Egyptians by terrorists belonging to the Gamat al-Islamiya (Islamic Group) at the Temple of Queen Hatsheput in Luxor, Egypt; and,

- the bombings of the U.S. embassies in Kenya and Tanzania in August 1998that killed 257 and injured some 5,000 others.

As the above incidents suggest, terrorism motivated in whole or in part by religious imperatives has often led to more intense acts of violence that have produced considerably higher levels of fatalities——at least compared to the relatively more discriminate and less lethal incidents of violence perpetrated by secular terrorist organizations.[33]

The reasons for the higher levels of lethality found in religious terrorism may be explained by the radically different value systems, mechanisms of legitimization and justification, concepts of morality, and Manichean world view that the religious terrorist embraces compared with his secular counterpart.[34] For the religious terrorist, violence first and foremost is a sacramental act or divine duty executed in direct response to some theological demand or imperative. Terrorism thus assumes a transcendental dimension,[35] and its perpetrators are thereby not affected by the political, moral, or practical constraints that seem to affect other terrorists. Whereas secular terrorists generally consider indiscriminate violence immoral and counterproductive,[36] religious terrorists regard such violence not only as morally justified, but as a necessary expedient for the attainment of their goals or as an inherently defensive response to a predatory or aggressive state, hostile society or rival religious group.

---

33 See Enders and Sandler, "Is Transnational Terrorism Becoming More Threatening? A Time Series Investigation," p. 21 where they argue, "This "shift toward greater religious-based terrorism is traced to the [1979] take-over of the US Embassy in Tehran, from which point terrorism became more casualty prone and dangerous." See also, Mark Juergensmeyer, "Terror Mandated By God," *Terrorism and Political Violence*, vol. 9, no. 2 (Summer 1997), pp. 16-23.

34 See the comparative discussion of the secular and religious terrorist mindset and legitimizing measures in Bruce Hoffman, "The Contrasting Ethical Foundations of Terrorism in the 1980s." *Terrorism and Political Violence*, vol. 1, no. 3 (July, 1989), pp. 361-377.

35 See, for example, Rapoport, "Fear and Trembling: Terrorism in Three Religious Traditions," p. 674.

36 Jenkins, *The Likelihood Of Nuclear Terrorism*, pp. 4–5.

Religion therefore serves as a legitimizing force——conveyed by sacred text or imparted via clerical authorities claiming to speak for the divine. This explains why clerical sanction is so important to religious terrorists, and why religious figures are often required to bless (e.g., approve) terrorist operations before they are executed. For example, the group of Jewish messianic terrorists who, in 1984 plotted to blow up The Dome of the Rock in Jerusalem (Islam's third holiest shrine) in hopes of provoking a cataclysmic, nuclear "holy war" that would result in the obliteration of all Israel's Arab enemies,[37] had made it clear to their leaders that they could not implement the groups' battle plan without specific rabbinical blessing.[38] Similarly, the World Trade Center bombers specifically obtained a *fatwa*, or religious edict from Sheikh Omar Abdel-Rahman (who is now also imprisoned in the United States) before planning their attack.[39] In the case of the American Christian white supremacists, the leaders of these groups are often themselves clergymen——like the Michigan Militia's[40] founder and "general", *Pastor* Norman Olson, the Idaho-based Aryan Nations' leader, *Reverend* Richard Girnt Butler and, the Ku Klux Klan's *Pastor* Thom Robb——who deliberately cloak themselves with clerical titles in order to endow their organizations with a theological veneer that condones and justifies violence.

Clerical sanction, if not blessing, also plays a critical role in the concept of martyrdom present in many religious terrorist movements. Muslim clerics have also lent their support and even encouraged as well as given their blessing even to self-martyrdom——though suicide is forbidden by Islamic law. For example, immediately after the 1983 suicide attacks on the U.S. Marines and French paratroop headquarters by the Lebanese Shi'a terrorist organization, Hezbollah, Hussein Mussawi, a leader of the group,

---

37 See Thomas L. Friedman, "Jewish Terrorists Freed By Israel," *New York Times,* 9 December 1984; Grace Halsell, "Why Bobby Brown of Brooklyn wants to blow up Al Aqsa," *Arabia,* August 1984; Martin Merzer, "Justice for all in Israel?" *Miami Herald,* 17 May 1985; and, "Jail Term of Jewish terrorist reduced," *Jerusalem Post* (International Edition), 12 October 1985. The information pertaining to the terrorists' desire to provoke a cataclysmic holy war between Moslems and Jews was verified by an American law enforcement officer involved with the investigation of Jewish terrorist incidents in the U.S. and knowledgeable of the Jerusalem incident in conversation with the author.

38 See Ehud Sprinzak, *The Ascendance of Israel's Radical Right* (New York & Oxford: Oxford University Press, 1991), pp. 98-99.

39 See Youssef M. Ibrahim, "Muslim Edicts Take on New Force," *New York Times*, 12 February 1995.

40 One of the groups with whom Timothy McVeigh, the accused Oklahoma city bomber, allegedly had close links.

said: "I proclaim loud and clear that the double attack of Sunday is a valid act. And I salute, at Death's door, the heroism of the kamikazes, which they are; they are now under the protection of the All Powerful one and of the angels."[41] This same ethos of self-sacrifice and suicidal martyrdom can be seen in many Sunni Islamic——and indeed other religious——terrorist organizations today——including al Qaeda, various Pakistani jihadi organizations, the Palestinian groups Hamas and Palestine Islamic Jihad, and so on. Violence in this context ineluctably is a sacramental act: a divine duty, commanded by religious text and communicated by clerical authorities. It is therefore meant not only to vanquish one's enemies but to assure the perpetrator ascent to a reputedly glorious heaven.

Finally, religious and secular terrorists also have starkly different perceptions of themselves and their violent acts. Where secular terrorists regard violence either as a way of instigating the correction of a flaw in a system that is basically good or as a means to foment the creation of a new system, religious terrorists see themselves not as components of a system worth preserving but as "outsiders," seeking fundamental changes in the existing order. This sense of alienation also enables the religious terrorist to contemplate far more destructive and deadly types of terrorist operations than secular terrorists, and indeed to embrace a far more open-ended category of "enemies" for attack: that is, anyone who is not a member of the terrorists' religion or religious sect. This explains the rhetoric common to "holy terror" manifestos describing persons outside the terrorists' religious community in denigrating and dehumanizing terms as, for example, "infidels," "dogs," "children of Satan" and "mud people." The deliberate use of such terminology to condone and justify terrorism is significant, in that it further erodes constraints on violence and bloodshed by portraying the terrorists' victims as either subhuman or unworthy of living.

The radical Sikh separatist movement as it emerged in the 1980s would appear to conform to this pattern and the characteristics of terrorism motivated or inspired by religious imperatives in a number of significant ways.[42] Professor Mark Juergensmeyer of the University of California at Santa Barbara is among the world's leading scholars and experts on violent religious militancy and arguably the doyen of this sub-field of

---

41 Quoted in draft copy of the United States Department of Defense Commission on the Beirut International Airport (BIA) Terrorist Act of October 23, 1983 (known as 'The Long Commission' in reference to its chairman, retired Admiral Robert L. J. Long, US Navy), p. 38.

42 Babbar Khalsa, the militant Sikh organization implicated in the bombings of the Air India aircraft, described by one writer as "one of India's largest terrorist organizations," was reportedly registered in Canada as a charity and a non-profit religious group. See Stewart Bell, *Cold Terror: How Canada Nurtures And Exports Terrorism Around The World* (Toronto: John Wiley & Sons, Ltd., 2007), p. 24.

terrorism studies. A specialist trained in the religions of south Asia, Professor Juergensmeyer has written or edited three seminal works on religion and terrorism: *Terror in the Mind of God, The New Cold War? Religious Nationalism Confronts the Secular State,* and *Violence And The Sacred In The Modern World.* Each of these path-breaking works discusses the phenomenon of Sikh religious militarism, its intellectual and theological roots and the growing militancy that sparked a dramatic escalation of seditious and inter-communal violence in India during the 1980s. Professor Juergensmeyer's description of the Sikh movement as having become intrinsically a religious-nationalist one fits very comfortably with the core characteristics of religious terrorism described above. In his analysis, even if previous, historical campaigns for autonomy and a greater voice and control over Sikh affairs were perhaps more political in character, the Sikh movement that this ferment produced in the 1980s was clearly "more intense, more religious" than its predecessor[43] with its fundamental objective the attainment of political legitimacy for Sikh identity—religious nationalism."[44] Indeed, Juergensmeyer charts the rise of Jarnail Singh Bhindranwale, the leader of that generation of militant Sikhs, from the time he was "a young rural preacher who at an early age had joined the Damdami Taksal, a religious school and retreat center founded by the great Sikh martyr Baba Deep Singh" and eventually became its head.[45] He reportedly was especially contemptuous of those whom Bhindranwale termed "the enemies of religion."[46] Thus, for Juergensmeyer the Sikh case is indisputably one of "religious legitimization" and he explains cogently how its nationalist and irredentist objectives became entwined with an overriding religious identity and justification. "One political demand, however, was not widely supported at the outset," he writes,

> and it desperately needed all the legitimization that it could get, including the legitimacy it could garner from religion. This was the demand for Khalistan, a separate Sikh nation. Although it was seen initially as a political solution to the Sikhs' desire for a separate identity, it soon became a religious crusade.[47]

---

43 Mark Juergensmeyer, *Terror in the Mind of God* (Berkeley; Univ. of California Press, 2000).
44 Mark Juergensmeyer, *The New Cold War? Religious Nationalism Confronts the Secular State* (Berkeley; Univ. of California Press, 1994), p. 95
45 Juergensmeyer, *The New Cold War?*, p. 94
46 Juergensmeyer, *Terror in the Mind of God*, p. 172.
47 Juergensmeyer, *The New Cold War?*, p. 163.

In sum, therefore, "the instrument of religious violence," Juergensmeyer concludes, "gave power to those who had little power before."[48]

The separatist element of the Sikh's nationalist and religious self-identification, other scholars have argued, is a reflection of that movement's hybrid character. A modern day offshoot of a Hindu reform movement founded in the Punjab some 400 years ago, the Sikhs are therefore an amalgamation of different beliefs and practices that, it is argued, lack a strong theology of their own. As such, the Sikh faith has long struggled to differentiate itself and its followers from Hinduism, placing a strong emphasis on prominent religious symbols and means of personal identification involving the Golden Temple at Amritsar and sacred scriptures as well as individual accoutrements such as the wearing of the turban, long hair and beards, and carrying a dagger.[49] Foremost among the Sikh's aims, therefore, became the establishment of a revitalized Sikh nation, called Khalistan——literally, "Land of the Pure."[50] Indeed, Juergensmeyer's analysis emphasizes this same point. The militant Sikh movement of the 1980s, he writes, "wanted the Punjab to include only speakers of the Punjabi language, a demand that was tantamount to calling for a Sikh majority state. . . . Soon Bhindranwale became busy with a new organization, the Dal Khalsa ("the group of the pure").[51]

In this regard, Sikhs embarked on a campaign to cleanse the Punjab of "foreign influences."[52] Bands of young Sikhs, for instances, started locally, indiscriminately killing Hindus, but 1981 appreciably escalated and broadened their campaign both tactically and geographically with the hijacking in Pakistan of an Indian Airlines plane. "The serious violence," Juergensmeyer notes, "had begun."[53] Indeed, it exploded on 5 June 1984, when India's Prime Minister, Indira Gandhi, ordered Indian forces to assault the Golden Temple, the Sikh's holiest shrine, to break the back of

---

48 Ibid, p. 169.

49 Bernard Imhasly, "A Decade of Terrorism in the Punjab," Swiss Review of World Affairs, March 1991 p. 23.

50 Ian Grieg, "The Punjab: Plagued By Terror," *Conflict International*, July 1992.

51 Juergensmeyer, *Terror in the Mind of God*, p. 97.

52 An estimated 20,000 persons were killed as a result of the violent campaign in the Punjab that followed. In 1991 alone, a record 4,700 deaths occurred in the Punjab. Although the majority of fatalities were members of the region's Hindu minority population, fellow Sikhs judged as traitors or apostates were also targeted (whom Bhindranwale termed "the enemies of religion") were also targeted. The Sikh attacks, one contemporary observer noted, were almost "entirely indiscriminate in nature," with crowded passenger trains a favorite target. One hundred Hindu passengers were killed and 70 injured in two such attacks in 1991. See Ian Grieg, "The Punjab: Plagued By Terror," *Conflict International*, July 1992.

53 Juergensmeyer, *Terror in the Mind of God*, 98.

the militant movement. Code-named "Operation Bluestar," the effort was neither neatly nor easily executed in any kind of a swift, surgical, timely manner. It took two, blood-soaked days to quell the violent resistance which the Indian Army encountered and which claimed the lives of more than 2,000 persons——including innocent worshippers. Bhindranwale was among the first to die in the assault and achieve the venerated status of a fallen martyr. As Juergensmeyer recounts, "Even moderate Sikhs throughout the world were horrified at the specter of the Indian army stomping through their holiest precincts with their boots on, shooting holes in the temple's elaborate marble facades." Vengeance for this blasphemous act was achieved less than six months later when two of Mrs. Gandhi's Sikh bodyguards assassinated her. Her murder begat a new spiral of inter-communal violence that commenced the following day, when rampaging crowds in Delhi and elsewhere murdered more than 2,000 Sikhs.[54] In retrospect, the chain of events that led ultimately to the acts of retaliation on 23 June 1985 merely perpetuated a cycle of anti-state, inter-communal violence that fed off itself seems clear. In rallies at New York's cavernous Madison Square Garden and elsewhere febrile calls for revenge and sacrifice fueled and sought to justify sectarian (e.g., anti-Hindu and anti-India) violence. In *Cold Terror*, Canadian journalist Stewart Bell recounts how a Canadian-Sikh named Ajaib Singh Bagri incited such sentiments. "When the blood of martyrs is spilled," Bagri reportedly began his speech, "the destiny of communities is changed. . . . Any speaker from here who will say 'Hindus are brothers' will be deemed a traitor to the community," he continued.

> 'Death to . . .' the audience shouted.
> 'Traitors of the natin!' yelled the slogan raiser, who leads the congregation in chants.
> 'Will create Khalistan . . . '
> 'Will sacrifice ourself.'
> 'Will create Khalistan . . .'
> 'For the retribution of sacrifices.'[55]

The indiscriminate nature of the Sikh violence is a common theme in religiously-motivated terrorism, reflecting the Manichean and passionately embracing extremes of good and evil with no middle gradation, nuance or subtlety. It is clearly present both in Sikhism and Bhindranwale's

---

54 Juergensmeyer, *The New Cold War?*, pp. 95-96. See also Bell, *Cold Terror*, p. 24.
55 Quoted in Bell, *Cold Terror*, pp. 23-25.

philosophy. Bhindranwale reportedly preached the Sikh concept of *miri-piri*——that spiritual and temporary power are linked. Thus, according to Juergensmeyer Bhindranwale "projected the image of a great war between good and evil waged in the present day"[56] that Bhindranwale, in his words, depicted as "a struggle . . . for our faith, for our Sikh nation, for the oppressed."[57]

Part and parcel of this Manichean world-view common to religious terrorists is the sense of exclusion and of an "us versus them" conflict; with the aggrieved religious movement conceiving their violence as an entirely defensive reaction——a last resort, by reluctant warriors, against a repressive state or predatory rival people. The Sikh religion, for instance, extols non-violence and condemns the taking of a human life. According to Juergensmeyer "Even Bhindranwale acknowledged that 'for a Sikh it is a great sin to keep weapons and kill anyone.'" At the same time, however, Bhindranwale maintained that violence was justifiable in "extraordinary circumstances"[58] "It is an even greater sin to have weapons and not seek justice," Bhindranwale explained in justification.[59] Another Sikh militant leader, Sohan Singh, who led the eponymous militant Sikh group that played an important coordinating role, the Sohan Singh Panthic Committee, expounded a similar justification for what would be deemed defensive violence. "If others try to kill you, you are warranted in trying to kill them," Sohan Singh told Juergensmeyer in an interview. Sohan Singh further argued that the "violence of the Sikhs in recent years was primarily a response to the violence of the state" and maintained that the "killings undertaken by militants were always done for a purpose; they were 'not killing for killing's sake.'" Most important, Sohan Singh claimed, "warnings were given and punishment was meted out only if the offenders persisted in the conduct that the militants regarded as offensive."[60] As Juergensmeyer observes,

The rhetoric of warfare is as prominent in modern religious faiths. The rhetoric of warfare is as prominent in modern religious vocabulary as is the language of sacrifice, and virtually all cultural metaphors are filled

---

56 Juergensmeyer, *Terror in the Mind of God*, p. 98

57 Jarnail Singh Bhindranwale, "Two Lectures." Given on 19 July and 20 September 1983, translated from the videotaped originals by R.S. Sandhu, and distributed by the Sikh Religious and Educational Trust, Columbus, Ohio. Martyrdom was the supreme honor bestowed quoted in Juergensmeyer, *The New Cold War?*, p. 92.

58 Juergensmeyer, *The New Cold War*, p. 164

59 Quoted in Ibid.

60 Juergensmeyer, *Terror in the Mind of God*, p. 99.

with martial metaphors. The ideas of a Salvation Army in Christianity and a Dal Khalsa ('Army of the faithful') in Sikhism, for instance, are used to characterize a disciplined religious organization.[61]

The Sikh extremists who mobilized in the 1980s to battle the Indian state thus also saw themselves as reluctant warriors, indeed, martyrs fighting to preserve their religious community against an exponentially more powerful, malevolent force. "The history of Sikhism," Juergensmeyer writes "is also one of violent encounters, usually in the defense of the tradition against its forces."[62] In no dimension of their struggle is this self-perception clearer than in the Sikh's embrace of martyrdom. Indeed, Juergensmeyer argues that "Martyrdom was the supreme honor bestowed on those who gave their lives to the cause.[63] In fact, he believes that it was the devotional Hinduism that flourished in a region of northern India dominated by Muslim rule, [which] may well have been influenced by the Islamic notion of martyrdom. The concept is central to the faith. One of the ten gurus who founded the tradition——Guru Tegh Bahadur——is perceived as a martyr to hostile Mogul forces and many of the most glorified heroes in Sikh history were martyred as well. One of these was Baba Deep Singh whom modern religious artists portray as being so valiant in his struggle against the forces of Sikhism that he fought on even after his head was severed from his body. With such a reputation, it should not be surprising that the most recent leader of the order founded by him to became a martyr as well. Baba Deep Singh's spiritual descendent, Jernail Singh Bhindranwale, led a militant band of Sikhs in a seemingly suicidal mission against Prime Minister Indira Gandhi; he was himself killed in her army's invasion of Sikhism's major shrine, the Golden Temple at Amritsar. In retaliation, Mrs Gandhi was assassinated——some pious Indians would say martyred——a few months later.[64]

The last words of two Sikh militants who assassinated an Indian general clearly exemplify the martyrdom concept that sustains and fuels many terrorist groups, but religiously-motivated or inspired ones in particular. The two assassins were reported to have described the hangman's noose awaiting them "as the embrace of a lover," explaining that they "longed for death as the martial bed" with their "dripping blood . . . the outcome of this union [that would] fertilize the fields of Khalistan.[65]

---

61 Mark Juergensmeyer, "Sacrifice and Cosmic War," in Mark Juergensmeyer (ed.), *Violence And The Sacred In The Modern World* (London: Frank Cass, 1992), p. 106.
62 Juergensmeyer, *Terror in the Mind of God*, p. 95.
63 Juergensmeyer, *Terror in the Mind of God*, p. 96.
64 Juergensmeyer, "Sacrifice and Cosmic War," pp. 103-104.
65 Quoted in Juergensmeyer, *Terror in the Mind of God*, p. 203

Intelligence and Law Enforcement

The fundamental expectation of all citizens everywhere is that their government will protect and defend them against threats and violence both internal and external. Historically, this compact between the people and their government has been assured by a traditional division of labor between law enforcement——that is, the police, who are responsible for domestic security through the upholding of the law and maintenance of order; and, the military——who are responsible for national defense, mostly against foreign threats. Sitting astride the two, with responsibility for domestic and foreign information-gathering as well as the grey area in-between when internal threats to security have external origins, are a country's intelligence services. The complexity of their roles and missions and more problematical jurisdictional demarcations is evidenced by the multiple intelligence agencies most countries maintain.

The military intelligence, police intelligence, and national intelligence agencies within a single country, for instance, frequently exist as separate entities, usually for separate purposes. These agencies' missions, training and *modi operandi* are different, although cooperation and coordination among and between them is essential.[66] National intelligence is often divided between external threats and internal, domestic threats: although it is difficult to compartmentalize when terrorists have a presence or conduct operations within a country from foreign bases or overseas sanctuaries. Military intelligence tends to be up-to-the-minute operational information geared to discerning enemy orders of battle and intentions or to acquiring essential information for force protection, thereby either preventing and thwarting attacks on military targets and personnel. Police intelligence, by contrast, involves the social, economic and——particularly when terrorism is involved——political information that defines the criminal operational environment that the authorities within a country must penetrate. Police intelligence has a special responsibility to adhere firmly to the rule of law if the information obtained to solve or prevent a crime is to be transformed into evidence admissible in a court of law.

---

66 More than often than not, however, bureaucratic competition and institutional rivalry between these services in fact inhibit, if not undermine, effective cooperation coordination. See Bruce Hoffman and Jennifer Morrison Taw, "A Strategic Framework for Countering Terrorism" in Fernando Reinares (ed.), *European Democracies Against Terrorism: Governmental policies and intergovernmental cooperation* (Aldershot, UK: Ashgate Dartmouth, 2000), pp. 15-16.

In responding to terrorist threats within a country, both "environmental" and operational intelligence are clearly necessary if the authorities are to be able to identify and apprehend terrorists concealed within the population at large or specific communities in particular and then to engage them successfully with arrest, trial, conviction, and sentencing or, in those cases when it is unavoidable, the application of deadly force in justifiable circumstances: without violating the law and/or alienating or negating the confidence and support of the public. In the liberal-democratic state this entails a delicate balancing act. Concern over civil liberties violations, for example, will often make domestic intelligence-gathering more difficult than foreign intelligence acquisition. Moreover, effectively sharing and disseminating that information with other government agencies outside the intelligence community can be especially challenging. There is the additional challenge of how to deal with intelligence that has been collected to a different standard from that used by law enforcement in the context of criminal prosecutions. Sensitivity to intelligence sources and methods with respect to how and from whom this information was obtained is an especially salient issue. One the one hand, those officials responsible for the collection of that intelligence will be reluctant to have its provenance in open court. On the other hand such information——however truthful and accurate——may not be legally admissible on various grounds whether as hearsay or because it is otherwise impossible to corroborate. Such concerns if not properly balanced can severely impact operational, counterterrorist capabilities. In some instances, they may also constrain the ability to pre-empt, prevent and resolve terrorist threats and/or undermine public confidence in the government and support for the authorities because of a perception of undermining or threats to civil liberties.

Terrorism thus presents a particularly acute dilemma regarding the need to preserve fundamental civil liberties on the one hand and protect society from attack or from the threat of enigmatic attack by clandestine adversaries. The challenge of effecting this balance was cogently described by Roy Jenkins, the United Kingdom's Home Secretary at the height of the violence in Northern Ireland during the early 1970s. "Governments," he observed, "must find a way to steer between two dangers; the first of failing to take effective and practical steps to deal with terrorism and the second of over-reacting and seriously damaging respect for human freedom and dignity."[67] The clandestinity, impenetrability, organizational

---

67 *The Times* (London), December 24, 1986 quoted in Bruce Hoffman and Jennifer Morrison Taw, *A Strategic Framework for Countering Terrorism and Insurgency* (Santa Monica, CA: RAND, 1992, N-3506-DOS), p. 51.

sophistication, and scope of terrorist operation thus necessitate that the authorities have the necessary (in some circumstances, extraordinary) legal powers to identify, monitor, arrest and prosecute terrorists and thereby neutralize this unique threat to society. At the same time, however, these powers must be exercised and overseen in such a manner that any infringement on civil rights is avoided. In sum, law enforcement and domestic intelligence officers must be given the legal tools they require to do their job while all the while balancing the security imperative with the need to avoid violating or infringing upon civil rights. The key to attaining this proper balance was summed by Ambassador Henry A. (Hank) Crumpton, who until recently was the senior U.S. Department of State official responsible for counterterrorism and whose prior career was as a long-serving Central Intelligence Agency operative. Although written within the context of post-9/11 security issues and terrorist threats to the United States, Ambassador Crumpton's words are relevant to other liberal-democratic states confronted with similar dilemmas. "U.S. intelligence and the American public," he wrote, must also both resolve a paradox. Intelligence must adhere to fundamentals of its craft, secretly protecting sources and methods while reaching beyond its traditional boundaries to build interdependence with American society. For their part, American citizens need to guard law and democracy fiercely, while seeking to understand and support internal intelligence collection against foreign enemies. If it is done correctly, domestic intelligence will not undermine democracy or civil liberties; if not, intelligence structures will devolve into pseudo-security mechanisms that serve the ruling powers at the expense of citizens.[68]

Regardless of the type of crime,information is required concerning all criminal acts which will aid in their solution, followed by identification, arrest, prosecution and conviction of the perpetrators. In this respect, the greatest similarities may be found in organized crime and terrorism since both involve networks of like-minded individuals functioning within some defined operational framework where security is essential to preserve both the organization's integrity and the resiliency or continuance of its operations——embracing, respectively, profit-making and political goals. Each, accordingly, must maintain a level of security that facilitates the conduct of effective transactions, whether financial or informational.

---

68 Henry A. Crumpton, "Intelligence and Homeland Defense" in Jennifer E. Sims and Burton Gerber (eds.), *Transforming U.S. Intelligence* (Washington, D.C.: Georgetown University Press, 2005), p. 198.

Therefore, it is imperative for both types of organization to avoid penetration by government spies and prevent potential informants from gaining access to vital information. Equally, they both must ensure that there are no witnesses to their activities from outside their organizations who might report to the authorities what they may have seen or heard and thus testify in a court of law. "Each type of organization," Philip B. Heymann, a former Deputy Attorney General of the United States and currently James Barr Ames Professor of Law at Harvard Law School, explains in his seminal treatise on this issue, *Terrorism and America: A Commonsense Strategy for a Democratic Society*, does its best to make it extremely difficult for the government to obtain accomplice witnesses, by choosing members carefully, rigorously controlling dissemination of information, and employing ruthless intimidation. Both types of organization make it difficult to obtain victim witnesses. In one case, because the victims are generally either willing participants in a crime, such as buyers of illegal goods or services, or frightened victims of extortion; in the other case, for similar reasons or because the crimes, such as placing a bomb to explode at a later hour, do not easily allow matching the crime with the criminal.[69]

Further, both organized criminal acts and terrorism present serial threats to society. That is, their crimes and violence are not isolated, much less spontaneous instances of rage, greed, or avarice, but planned, premeditated and conspiratorial deeds designed to further their organizations' goals (whether financial or political) and ensure its continued vitality, viability and resiliency. In this respect, the resources and capabilities required to sustain either an organized criminal enterprise or a terrorist campaign extend beyond the requirements to commit a single crime and are at once as conspiratorial as they are instrumental. Indeed, in some cases the capabilities and sophistication of either organized criminal or terrorist entities may rival, if not even eclipse, those of governments and established nation-states. Finally, in order to preserve themselves and protect their operations, both organized criminal gangs and terrorist organizations often engage in energetic and wanton intimidation of witnesses. "In both cases" Heymannn continues, prosecutors, judges, and lay fact-finders can be subjected to intimidation; being a judge or a prosecutor in an organized crime case in Palermo or Bogota is hardly safer than being a

---

69 Philip B. Heymannn, *Terrorism and America: A Commonsense Strategy for a Democratic Society* (Cambridge, MA: MIT Press, 1998), p. 113.

judge in a terrorist case in Belfast. In both cases the organization may enjoy equipment and resources far superior to that of the ordinary criminal.[70]

Thus it is not surprising that over the past decade, national intelligence agencies and security services provided increasing assistance to law enforcement agencies in investigating serious crimes, especially when cross border and even international operations were involved. This process was accelerated by two developments in the 1990s: the end of the Cold War, that freed up often highly sophisticated and technologically advanced signals intelligence (SIGINT) capabilities and enabled the re-deployment of formidable human intelligence (HUMINT) activities to countering organized criminals. Also the emerging "globalization" phenomenon that had re-written the rules and conduct of trans-national commerce and communication, and thereby presented new opportunities to multi-national criminal and narcotics syndicates which navigated equally deftly between state borders and cracks in domestic governance.[71] As Michael Herman, who until his retirement, occupied a number of senior and very sensitive coordinating posts in the British intelligence establishment, explains, intelligence in this context involves some special efforts at collection but is related mainly to the coordination and study of information in depth from all sources; it 'targets the criminal rather than the crime.' Its output is assessments and forecasts geared to assist action at all law-enforcement levels, from the pursuit of particular cases to strategic decisions about the deployment of law enforcement effort. Organized law enforcement intelligence of this kind is therefore becoming a parallel to the government intelligence system . . . ."[72] Of course, the financing of terrorism has long produced marriages or alliances of convenience between terrorists and criminals when a commonality of interests and profit were present. This, however, is discussed in the following section. But, these similarities notwithstanding, the differences between fighting organized crime and combating terrorism are as profound as they are formidable. Terrorism differs markedly from criminal activity in its impact on society. Admittedly, like terrorists, criminals use violence as a means to attaining a specific end. However, while the violent act itself may be similar——murder, kidnapping, extortion, and arson, for example——the purpose or motivation clearly is not. Whether the criminal employs violence as a means to obtain money, to acquire material goods, or to kill or injure a

---

70 Heymannn, Terrorism and America, p. 113.

71 Michael Herman, *Intelligence Power In Peace And War* (Cambridge: Cambridge University Press, 1996), p. 348.

72 Ibid., p. 350.

specific victim for pay, he is acting primarily for selfish, personal motivations (usually material gain). Moreover, unlike terrorism, the ordinary criminal's violent act is not designed or intended to have consequences or create psychological repercussions beyond the act itself. The criminal may of course use some short-term act of violence to "terrorize" his victim, such as waving a gun in the face of a bank clerk during a robbery in order to ensure the clerk's expeditious compliance. In these instances, however, the bank robber is conveying no "message" (political or otherwise) through his act of violence beyond facilitating the rapid handing over of his "loot." The criminal's act therefore is not meant to have any effect reaching beyond either the incident itself or the immediate victim. Further, the violence is neither conceived nor intended to convey any message to anyone other than the bank clerk himself, whose rapid cooperation is the robber's only objective. Perhaps most fundamentally, the criminal is not concerned with influencing or affecting public opinion: he simply wants to abscond with his money or accomplish his mercenary task in the quickest and easiest way possible so that he may reap his reward and enjoy the fruits of his labours. By contrast, the fundamental aim of the terrorist's violence is ultimately both broader and more profound. From attempting to alter fundamentally the socio-economic and political condition of a country to achieving signal changes in a country's domestic or foreign policies or simply as a means to call attention to the terrorists and their cause——all of these issues concerning which the ordinary criminal couldn't care less, of course.[73] As Herman argues, "However criminal it may be, terrorism is the use of violence for political and not for other purposes. Broadly speaking there are different interests and objectives in both targets and the intelligence coverage of them."[74] Heymann picks up this same point but usefully expands to note how, Part of the answer to why it has appeared necessary to change the rules of law enforcement far more in the case of terrorism is found in the fact that terrorism arouses public fears and anger much more than even organized crime. Still, there are also two real differences. The first . . . [is] the special difficulty of narrowing the list of suspects into a manageable number is compounded in the case of terrorism. Beyond this, the stakes of bringing terrorist activity to a close are often much higher than the stakes in bringing organized crime or ordinary crime to a close. Terrorism often threatens a continuing course of violence and death. Nor are the victims, as in the case or organized crime,

---

73 Konrad Kellen, On Terrorists and Terrorism (Santa Monica, CA: RAND Corporation, N-1942-RC, December 1982),p. 9. See also, the discussions in Herman, Intelligence Power In Peace And War, p. 351; and, Heymannn, Terrorism and America, pp. 112-113

74 Herman, Intelligence Power In Peace And War, p. 351.

likely to be inside participants with some responsibility for the danger they confront. Faced with the threat of continuing random violence, a nation may conclude that stopping the course of terrorist violence is simply more important, and arouses stronger public demands, than catching people who have committed other crimes, even the leaders of organized vice.[75]

Indeed, in the post-9/11 world, the threat of terrorism to the nation-state not infrequently spoken of in existential terms: particularly with respect to the potential terrorist use of some weapon of mass destruction (WMD). As Walter Laqueur, one of the founding fathers of the field of terrorism studies, warned in a seminal reassessment of terrorism trends and thinking published in 1996, "Proliferation of weapons of mass destruction does not mean that most terrorists are likely to use them in the foreseeable future, but some almost certainly will, in spite of all the reasons militating against it."[76] In this respect, it was bin Laden's alleged development of chemical warfare agents for use against U.S. forces in Saudi Arabia that was cited just two years later to justify the controversial American cruise missile attack on the al-Shifa pharmaceutical plant in Khartoum, Sudan.[77] Moreover, since that time incontrovertible information has repeatedly come to light that clearly illuminates al Qaeda's longstanding and concerted efforts to develop a diverse array of chemical, biological, and even nuclear weapons capabilities.[78] Thus, the unique threat posed by terrorism, and the extraordinary measures necessary to counter it, go beyond Heymann's arguments of a sustained and systematic campaign of violence to ones that could arguably challenge the well-being of a country and its populace.

Thus, it is not surprising that the state may require greater flexibility and special powers in dealing with the terrorist threat. Given that this particular type of threat will generally be more diffuse and more difficult to identify because of its inherent clandestinity and trans-national dimensions—— and, indeed, because its potential consequences could be exponentially

---

75 Heymannn, *Terrorism and America*, p. 113.

76 Walter Laqueur, 'Postmodern Terrorism,' *Foreign Affairs*, vol. 75, no. 5 (September-October 1996), p. 34.

77 See both the contemporary accounts of the explanation for the strike by Barbara Crossette, et al., "U.S.. Says Iraq Aided Production of Chemical Weapons in Sudan," *New York Times*, 25 August 1998; Michael Evans, "Iraqis linked to Sudan Plant," *The Times* (London), 25 August 1998; James Risen, "New Evidence Ties Sudanese To Bin Laden, U.S. Asserts," *New York Times*, 4 October 1998; Gregory L. Vistica and Daniel Klaidman, "Tracking Terror," *Newsweek*, 19 October 1998 and the "insider" account published by two members of President Clinton's National Security Council staff, Daniel Benjamin and Steven Simon, *The Age of Sacred Terror* (New York: Random House, 2002), pp. 259-262 & 353-365.

78 John Parachini, "Putting WMD Terrorism into Perspective," *The Washington Quarterly*, vol. 26, no. 4 (Autumn 2003), p. 44

more serious than in the past——the importance of intelligence to anticipate, pre-empt, and respond is paramount. Thus, intelligence has the potential to begin "scanning the horizon for potential threats." This monitoring or "patrolling of the environment" as Heymann describes it, would likely include, but not necessarily be limited to:

- scrutiny of persons entering or leaving a country;
- the purchase of unusual combinations or large amounts of chemicals, fertilizer (e.g., ammonium nitrate) or stocks of other legally available and commercially procurable materials that can be used to fashion a home-made bomb; and
- surveillance or reconnaissance of likely, potential targets, be it an iconic landmark, government facility, mass transit, nuclear power plant or an specific individual, etc.

"Mid-way between such a 'patrol' and knowing at least the existence of a violent group," Heymann goes on to explain, lies intelligence-gathering focused on individuals or groups that are more likely than others to embark on a course of political violence. Information may have come from abroad .... It may come in the form of a tip from a local informant. Or it might come from observing a social setting in which the necessity of violence for political purposes is preached and taken seriously.[79]

In these circumstances, increased emphasis on intelligence and in particular its pre-emptive and predictive roles even in a wholly domestic context is understandable. "Intelligence-gathering," Heymann——a jurist and former senior U.S. Justice Department official——thus argues, "is the most important form of prevention of terrorism."[80] This increased monitoring of the diverse potential range of threats should not——it bears being repeated——be at the expense or in violation of the fundamental civil liberties inherent in the liberal-democratic state——and there is no reason why it should be. There is already a depressing past record of excesses and violations that should serve as guideposts so as to ensure that past mistakes are not repeated and adequate controls, oversight, sunset clauses and other checks over intelligence and security services are firmly in place. At the same time, a middle course must be found that will effectively strike a balance between the protection of basic civil

79 Heymannn, *Terrorism and America*, pp. 130-131.
80 Heymannn, *Terrorism and America*, p. 156.

rights whilst endowing the state's intelligence and security agencies with the tools that will enable them to better anticipate and predict potential terrorist actions and thereby communicate them in a timely and cogent way to their political masters.[81] "The primary objective of intelligence-gathering," Heymann continues, is to deal with future danger, not to punish past crimes. As long as a group committed to political violence is at liberty, it poses a serious danger. This difference in primary purpose creates a difference in what information it is crucial to obtain. Prosecutors seeking conviction may have little interest in all but the first two of the following eight questions that are critical to prevention:

- Who are the members actively engaged in planning to use violence for political purposes?
- What is their motivation?
- Where are they located?
- Who in the population is likely to join the group or provide forms of support needed for its continued operations?
- What is the extent and nature of the support the group is receiving from others outside the country, including another state?
- How does the group handle the problems of remaining clandestine and yet carrying out political violence? What is its *modus operandi*?
- What type of attacks is the group capable of?
- What is the strategy behind their planning?[82]

Inevitably, the emphasis on intelligence's importance in countering terrorism brings into sharp focus the different missions and orientation of law enforcement and intelligence agencies. Writing in the early

---

81 See the discussion in Brian Michael Jenkins, *Unconquerable Nation: Knowing Our Enemy Strengthening Ourselves* (Santa Monica, CA: RAND Corporation, 2006), p. 170.

82 Heymannn, *Terrorism and America*, pp. 129-130.

1990s, Herman presaged the evolution of law enforcement into domains hitherto the provenance of national intelligence organizations,[83] including the posting of liaison police officers overseas such as the New York City Police Department has pioneered and the fusion centers linking not only federal, state and local enforcement entities together but other federal agencies, including intelligence services.[84] As Crumpton argues, in the post-9/11 worldthere are compelling reasons for law enforcement and intelligence to cooperate, to complement each other, and to overlap. First and foremost, the primary customer for domestic foreign intelligence on near-term threats is law enforcement And law enforcement can provide invaluable leads for intelligence officers. The intelligence collector and the law enforcement consumer, therefore, must strive for more than information sharing; they must seek interdependence.[85]

The main challenge, however, is the difference between information-gathering for intelligence——that is. the knowledge necessary to pre-empt or prevent a terrorist attack——and information-gathering designed to solve a case and therefore for introduction as evidence in a court of law. Indeed, this is also the fundamental difference between a police officer, who is trained in the rules of law and evidence, and an intelligence operative or analyst who generally is not. Arguably the most sensitive dimension of intelligence-gathering is the sources and methods used to obtain the information. Access to such details are generally very closely held and restricted on a "need to know basis." Evidence gathering about a crime is by definition collected to be shared: in the final result, in a court of law to obtain conviction. Intelligence is arguably only effective when it is not known publicly that it possessed. Heymann cogently delineates these key differences. "Every criminal investigation," he writes is an attempt to match what can be learned about a crime with information that can be learned about particular suspects, for purposes of prosecution in court. The way the information can be gathered——the investigative procedures——and the ways it can be used at trial are subject to a carefully devised set of rules.

Intelligence-gathering about a violent group has different purposes: to prevent political violence from occurring and to assist political leaders in

---

83 Herman, *Intelligence Power In Peace And War*, p. 350.

84 See, for instance, the Hon. Bennie G. Thompson, Member of Congress (D-MI), *LEAP: A Law Enforcement Assistance and Partnership Strategy: Improving Information Sharing Between the Intelligence Community and State, Local, and Tribal Law Enforcement* (Washington, D.C: Prepared at the Request of Congressman Bennie G. Thompson, Ranking Member, By the Democratic Staff of the Committee on Homeland Security, October 2006), passim.

85 Crumpton "Intelligence and Homeland Defense," p. 210.

responding to it in ways in addition to prosecution. The rules for gathering information and the regulations (systems of classification for keeping national security material secret) for its use may also differ from a criminal investigation. Where the rules for gathering information are more lenient than the rules for criminal investigations, it is because greater importance is attached to preventing violence from occurring and because, not being targeted toward particular suspects, the need for protection of individual rights may be less.[86]

Intelligence, therefore, looms ever more vital to the effective prevention and deterrence of terrorism today and in the future than it was in the past and is thus especially crucial with regard to these new threats. It is understandable why it is, and will likely remain, an undiminished and high priority for security and intelligence services, as well as law enforcement, everywhere.

Terrorist Financing Issues

One area of international terrorism that appears to have changed little between today and the 1980s is that of terrorist finances. Terrorists have long resorted to illegal revenue generating activities, including: fraud, extortion, kidnapping, smuggling (of both humans and commercial goods), narcotics and/or weapons trafficking, counterfeiting (both of money and consumer goods like music CDs and DVDs and VCR tapes of commercial films, tax avoidance, skimming of money from legal transactions (e.g., adjusting the weights and measures of purchases of gasoline) and from philanthropic donations made both knowingly and unknowingly to charities that serve as fronts for the terrorist group. In these respects, a variety of terrorists have long turned to Diaspora communities of their co-religionists or ethnic brethren for support and assistance: both passive and active, voluntary and coerced. Indeed, even if terrorist financing needs, procurement and practices have remained relatively unchanged over time, the involvement of Diaspora communities in funding terrorism has only grown and intensified over the past quarter century.

As in so much regarding the escalation of international terrorism since the late 1960s, the Palestine Liberation Organization (PLO) and individual Palestinian groups outside that organization's umbrella, have been an

---

86 Heymannn, *Terrorism and America*, p. 129.

inspiration and example to other terrorist movements elsewhere in terms of finance and revenue-generation, too.

The success achieved by the PLO in publicizing the Palestinians' plight through "internationalization" of its struggle with Israel has since served as a model for similarly aggrieved ethnic and nationalist minority groups everywhere, demonstrating how long-standing but hitherto ignored or forgotten causes can be resurrected and dramatically thrust onto the world's agenda through a series of well-orchestrated, attention-grabbing acts.[87] Some accounts suggest that by the early 1980s at least forty different terrorist groups——from Asia, Africa, North America, Europe and the Middle East——had been trained by the PLO at its camps in Jordan, Lebanon and the Yemen, among other places. The Palestinians' purpose in this tutelary role was not entirely philanthropic. The foreign participants in these courses were reportedly charged between US$5,000 and $10,000 each for a six-week program of instruction. In addition, many of them were later recruited to participate in joint operations alongside Palestinian terrorists. Thus, according to Israeli defense sources, the PLO in 1981 had active cooperative arrangements with some twenty-two different terrorist organizations that had previously benefited from Palestinian training, weapons supply and other logistical support.[88]

The PLO, though, was also one of the first terrorist groups actively to pursue the accumulation of capital and wealth as an organizational priority. Building on donations from Saudi Arabia and the other oil-rich Arab states in the Arabian Gulf and contributions made by individual Palestinians leaving in their peoples' large Diaspora across the Middle East, in Australia, Europe, South America, the United States and elsewhere, the PLO was able to amass a substantial nest egg. By the mid-1980s, it was estimated to have established an annual income flow of some US$600 million, of which some US$500 million was derived from investments.[89] The amassing of so vast a fortune is all the more astonishing given the fact that, when the PLO was established in 1964, it had no funds, no infrastructure and no real direction. It was not until the late Yasir Arafat's election as chairman in 1968 that the

---

87 Between 1968 and 1980, Palestinian terrorist groups were indisputably the world's most active, accounting for more *international* terrorist incidents than any other movement. During this time period they were responsible for 331 incidents compared with the 170 incidents attributed to the next most active group, the anti-Castro Cuban terrorist movements, and Irish and Turkish groups in third position with 115 incidents each (RAND Corporation Terrorism Databases).

88 James Adams, *The Financing of Terror* (New York: Simon & Schuster, 1986), p. 49.

89 Ibid., p. 243.

PLO started to become the major force in international politics that it is today. As the renowned former *Sunday Times* journalist and authority on terrorism James Adams has observed, as the PLO has grown in complexity and its income has risen accordingly, the organisation has had to adapt to a changing role and an altered image of itself. While the world still viewed the PLO as a bunch of terrorist fanatics robbing banks and blowing up aircraft to boost their cause, the secret side of the organisation was being rapidly transformed.[90]

Indeed, a decade after Arafat's ascent to chairmanship of the PLO, the movement was funding other terrorist groups and revolutionary movements. It was particularly generous to the newly-installed Sandinista regime in Nicaragua in the late 1970s and early 1980s. In November 1981, for example, the PLO made a US$10 million loaned the Sandinistas.[91] Additional loans amounting to US$12 million appear to have been made in succeeding years.[92] The PLO also played a leading role in the creation of a Nicaraguan national airline. In late 1979, the first of several Boeing 727 aircraft was reportedly donated by the PLO to Aeronica, the Nicaraguan airline.[93] The PLO's largesse in this regard led some sources to suggest that it owned 25 per cent of Aeronica.[94] And, after the United States cancelled US$75 million in economic aid to Nicaragua's private sector, the PLO arranged for a six-month $100 million loan from Libya.[95]

Nor was the PLO alone among Palestinian terrorist groups in either profits or financial acumen. The break-away, renegade splinter group, known formally as the Fatah Revolutionary Council, but more commonly as the Abu Nidal Organization (ANO) is a prominent case in point. Founded and led by the late Palestinian terrorist Sabri al-Banna, who had been variously employed by Syria, Iraq and Libya during the 1970s and 1970s, the ANO profited handsomely from this mercenary role. Indeed, as it became wealthier, the group progressively relinquished its original revolutionary/political motivations in favor of activities devoted almost

---

90 Ibid., p. 104.

91 Bruce Hoffman, "The PLO and Israel in Central America," *Terrorism and Political Terrorism*, vol. 1, no. 4 (October 1989), p. 488.

92 Ibid. See also, James Adams, "The Financing of Terror," *TVI Report*, vol. 7, no. 3 (Winter 1988), p. 31; David J. Kapilow, *Castro, Israel and the PLO*, (Washington, D.C.: The Cuban-American National Foundation, 1984), p. ; and, Eileen Scully, "The PLO's Growing Latin American Base," *The Heritage Foundation Backgrounder No. 281* (Washington, D.C.: The Heritage Foundation, 2 August 1983).

93 Adams, "The Financing of Terror," p. 31; and, Center for International Security, "The Sandinista PLO Axis: A Challenge to the Free World," *Spotlight on the Americas* (Washington, D.C.: CSIS, February 1984), p. 3

94 Adams, "The Financing of Terror," p. 31.

95 Ray Cline and Yonah Alexander, *Terrorism: The Soviet Connection* (New York: Crane Russak, 1984), p. 70. See also, Kapilow, *Castro, Israel and the PLO*, pp. 13 & 14.

entirely to making money. The ANO reputedly amassed a considerable fortune: initially through its "for-hire" terrorist activities, but then through exploiting its gains from these deals in shrewd commercial and real estate investments, including the profitable operation of a multinational arms trading company that had been based in Poland. In 1988 the ANO's assets were said to be worth an estimated US$400 million. Given the vast profits involved, not surprisingly the group's financial portfolio was administered by a separate "finance directorate" within the organization——with Abu Nidal himself at its head.[96]

If the PLO and ANO in the 1970s and 1980s provides an example of international terrorism gone corporate——with investments in real estate, airlines, hotels, stock portfolios and loans to foreign governments, the Provisional Irish Republican Army's (PIRA) activities over the same period evidences terrorism involvement in less genteel and more bare-knuckled money-making enterprises. Donations and Diaspora support——in this instance, from the Irish-American community——has been credited by PIRA with sustaining the conflict in Northern Ireland throughout the 1970s and 1980s. The extent of Irish-American support for the Republican cause is evidenced by the facts that at least half of PIRA's budget——especially for prisoner welfare and humanitarian assistance——raised in the U.S.[97] Further, 70% of PIRA weapons recovered in Northern Ireland were of American origin——a reflection of the belief that at least a fifth of PIRA's budget was dedicated to weapons purchases by agents operating from the U.S.[98] In sum, PIRA was believed to have generated US$2.5mn per annum thru the mid-1990s as a result of the fund-raising efforts of its U.S.-based NGO, NORAID ("Irish Northern Aid") and thereafter US$3.5mn a year for a total estimated in the neighborhood of US$50 million.[99]

---

96 Patrick Seale, *Abu Nidal: A Gun For Hire* (New York: Random House, 1992), pp. 202-5.

97 Adams, The Financing of Terror, p. 136

98 Andrew Wilson, *Irish America and the Ulster Conflict 1968-1995* (Belfast, Northern Ireland: Blackstaff Press, 1995), p. 290. See also the anecdotal, but detailed, description of PIRA arms procurement activities in the U.S. in Peter Taylor, *Provos: The IRA and Sinn Fein* (London: Bloomsbury, 1997), pp. 84-85.

99 Rohan Gunaratna, *International Terrorist Support Networks* (London: CSTPV Series in Terrorism & Political Violence and C. Hurst & Co., forthcoming). See also Gerard Hogan and Clive Walker, *Political Violence and the Law in Ireland* (Manchester & New York: Manchester University Press, 1989), p. 161.

PIRA's philanthropic income stream is supplemented by its manifold criminal activities in both Northern Ireland and the Republic of Ireland. Racketeering, kidnapping, fraud, extortion, illegal drinking clubs and taxi services, skimming money from gambling machines, tax evasion, video piracy and other low-level criminal activities also account for a large share of its budget. Given that the PIRA's annual operating costs were estimated in 1992 to be some £6 to 7 million pounds sterling (to pay for weapons purchases, salaries, legal fees, and welfare assistance to the families of deceased or imprisoned terrorists), the movement had to have diverse income streams.[100] The "bulk of their finance," one source argues came from bank and post office robberies both in Northern Ireland and the Republic. Police believe that this source of revenue amounted to some £700,000 in 1982 and 1983 alone.[101] A more recent robbery, of the main Belfast branch of the Northern Bank, netted the group some £26.5m—— about US$50 million.[102]

In the past, additional revenue has also been derived from kidnapping.[103] Among the victims were business, supermarket magnates and even the race horse, Shergar, owned by the Aga Khan. An estimated £1.5 million was netted from a spate of early 1980s abductions.[104] But these infrequent high value bank robberies and kidnappings apart, the mainstay of PIRA financing has been racketeering and other low-level criminal activities. The continuance and tolerance of such activities is a reflection of the PIRA's relationship with its constituency. "The Provisional IRA's well-developed fundraising structure," David McKittrick, arguably the province's leading journalist writes is based on a carefully worked-out philosophy. Its guiding principle is that it should be broadly acceptable in those Catholic working-class areas from which it draws support . . . . The IRA's methods are, in general terms, no great secret to most people in the republican ghettos; the emphasis is on ensuring that the techniques of raising money do not alienate actual or potential supporters.

---

100 Interview with Terrorism Finance Unit, Northern Ireland Office, Stormont Castle, Belfast, Northern Ireland, January 1992.

101 Brendan O'Brien, *The Long War: The IRA and Sinn Fein, 1985 to Today* (Dublin: The O'Brien Press 1993), p. 121.

102 Independent Monitoring Commission, *Fourth Report of the independent Monitoring Commission: Presented to the Government of the United Kingdom and the Government of Ireland under Articles 4 and 7 of the International Agreement establishing the Independent Monitoring Commission*, Ordered by the House of Commons to be printed 10th February 2005, HC 308 (London: The Stationery Office), p. 1, accessed at: http://www.independentmonitoringcommission.org/documents/uploads/HC%20308.pdf.

103 Hogan and Walker, *Political Violence and the Law in Ireland*, p. 162.

104 O'Brien, *The Long War*, p. 212.

For that reason, the PIRA's preferred revenue generation is to make money from the illegal drinking clubs, the unlicensed black taxis that serve them and the gaming machines scattered throughout the bars.[105] In addition, however, more intimidatory and coercive measures are employed——especially extortion of the construction and building trade.[106] Such activities are believed to net the PIRA thousands of pounds per week. A Northern Ireland businessman explained how it works.

Two of these men came into my office and explained very vividly, that I needed protection for my business When I said that I didn't want any, they replied that accidents could happen, that fires could start. . . .I went to the police and told them about the threats. They showed me mugshots and I picked out the two men immediately. They asked me if I would give evidence in court but they made it very clear they couldn't protect me or my family if I did.

The business withdrew his complaint and, presumably, paid the two terrorists the sum they demanded. He was doubtless influenced by a friend who had similarly been approached, but had rebuffed the offer of protection. Soon after, the friend received in the mail a photograph of himself, his wife and his children leaving church one Sunday. Yet another friend, whose interest in paying a "security retainer" had also been solicited, reported how his wife received a phone call stating only that, "Your son looked well getting out of school today." Such tactics in an environment where the authorities cannot provide witness protection, needless to say, are compellingly persuasive. As one victim explained, "They call at a site, or at a man's home and talk to his wife. The most effective thing they do is to mention his family; very often that's enough. They don't need guns or hoods."[107] Although weapons procurement, salaries and operational expenses account for the lion's share of PIRA expenditure, the large number of prisoners once held in Northern Irish jails was another drain on the movement's revenues. Each family, for instance, was paid a weekly contribution between £5 and 10 pounds. Given that Northern Ireland's prisons at one point held some 1,300 inmates convicted for terrorism-related offenses, PIRA's annual expenditure on what was termed "prisoner welfare," according to McKittrick, was "almost certainly in excess of £500,000."[108]

---

105 David McKittrick, Dispatches from Belfast (Belfast: Blackstaff Press, 1989), pp. 148-149.
106 Hogan and Walker, *Political Violence and the Law in Ireland*, p. 162.
107 Quoted in McKittrick, Dispatches from Belfast, pp. 146-147.
108 Ibid., p. 148

The Liberation Tigers of Tamil Eelam (LTTE or Tamil Tigers) fund-raising activities, however, are more heavily predicated on contributions——whether voluntary or coerced——from its Diaspora in Canada, Australia, the United Kingdom and elsewhere.[109] According to one source, in the 1990s the LTTE maintained offices in some 38 different countries that were charged with liaison and fundraising from a Diaspora of some 450,000 Tamil expatriates. Through a mixture of legitimate and illicit revenues, it was estimated at the time that the Tigers had an income estimated at US$24-100 million per year[110] (other estimates peg this figure more precisely to a sum of at least US$50,0000). It is further believed that some 60 percent of the LTTE's budget is raised in Europe and North America.[111] Four main income streams provide the movement's revenue:

- direct contributions from migrant communities;
- funds siphoned off contributions given to NGOs, charities, and benevolent donor groups;
- people-smuggling; and,
- investments made in legitimate, Tamil-run businesses.

All told, these activities conservatively furnish the LTTE with upwards of US$1.5 million per month. Most is derived through a "standard baseline 'tax" that is imposed, as a minimum obligation, on all families living in the respective host state." Canadian Tamils, for instance, were reported to be taxed at a rate of US$240 a year per household in 1999——"the equivalent of one Canadian dollar per day." Two years later, this figure was thought to have increased to $646——a roughly identical sum to the amount Tamils living in the United Kingdom were expected to pay (e.g., f300).[112] Like the PIRA, the Tigers, according to one source, prefer to procure this money voluntarily, relying on the effectiveness of positive publicity to galvanize contributors. When their solicitations fail to procure donations voluntarily, however, the Tigers quickly resort to intimidation and coercion: threatening family members who may remain in LTTE-controlled areas in Sri Lanka or threatening the unwilling contributors themselves.[113]

---

109 Daniel Byman, et al., *Trends in Outside Support for Insurgent Movements* (Santa Monica, CA: RAND Corporation, MR-1405-OTI, 2001), p. 50.
110 Gunaratna, *International Terrorist Support Networks.*
111 Ibid.
112 Ibid.
113 Byman, et al., *Trends in Outside Support for Insurgent Movements*, p. 51.

The effectiveness of these efforts may be seen in some of the estimates of Diaspora largesse: the more than 200,000 Tamils living in Canada are thought to have provided the LTTE with some US$730,000 per year.[114]

In addition to these "contributions," the LTTE also reportedly siphons off funds from donated to non-profit NGOS, relief organizations and other front organizations and also engages actively in both goods and human smuggling. A final income source is the revenue provided by legitimate businesses and commercial holdings.[115] These monies are used primarily to obtain arms, financing in the 1990s the purchase of 60 tons of RDX plastic explosive from the Ukraine and the diversion of 47,000 mortar shells purchased from the Sri Lankan Armed Forces from a Ukrainian dealer into the LTTE's hands.[116] As one source, explains, "The LTTE insurgency and its diaspora are intimately tied to one another. So long as the group can use its diaspora to raise funds, its guerrilla and terrorist campaign can be sustained."[117]

It remains only to consider al Qaeda——a subject impossible to ignore in a discussion of terrorism finances. Like the aforementioned terrorist movements, al Qaeda has also depended on an extensive fund-raising network involving charitable foundations, illicit activities such as smuggling, and investments in legitimate businesses and other legal commercial activities. Its finances and revenue generation was extensively examined by the 9/11 Commission (formally, the National Commission on Terrorist Attacks Upon the United States). Among al Qaeda's most important income streams was the donations Muslims are obliged to make as part of Islam's five core responsibilities. Called *zakat* in Arabic, al Qaeda was particularly adept at siphoning off these voluntary contributions for its own purposes. According to the 9/11 Commission, the movement "relied on a core group of financial facilitators who raised money from a variety of donors and other fund-raisers, primarily in the Gulf countries and particularly Saudi Arabia." Additional funds were obtained from the money collected by employees of either corrupt charities or ones with lax book-keeping practices.[118]

---

114 Ibid, p. 50

115 Ibid, pp. 51-52. See also the detailed discussion of LTTE activities in Canada by Bell, Cold Terror, pp. 47-102

116 Gunaratna, *International Terrorist Support Networks.*

117 Byman, et al., *Trends in Outside Support for Insurgent Movements*, p. 54.

118 *The National Commission on Terrorist Attacks Upon the United States, the 9/11 Commission Report*, (New York: W.W. Norton & Company, 2004)., 170.

Certainly, Usama bin Laden's personal fortune also played a large part in al Qaeda's founding, genesis and early operations. Further, his largesse was critical both in sustaining a number of Egyptian jihadi organizations that might not have survived without his help and in the construction of terrorist training camps in Afghanistan and the courses of instruction for foreign recruits who had traveled there in the late 1980s and early 1990s.[119] But, from the start, a variety of charitable organizations provided substantial financial support to al Qaeda. Donations for humanitarian assistance, for instance, was systematically siphoned off and applied to al Qaeda military activities: including training, recruitment, travel expenses, weapons purchases, etc. The case of Wadih el-Hage, who was bin Laden's personal secretary in Khartoum, was sent to Nairobi in 1994 to oversee al Qaeda operations in Kenya and begin the preparations for the 1998 bombing of the American embassy there. El-Hage's "cover" was as both a businessman and charity director. When not working as a gemstone dealer, for instance, el Hage managed Help African People, an NGO reportedly falsely registered as the local arm of a bona fide German charity. In this manner he was able to collect money and funnel it into Al Qaeda's coffers without detection. Bin Laden reportedly also used Human Concern International (HCI), an NGO he helped found during the Afghan jihad, to transport jihadi fighters from Bosnia to Sudan and elsewhere.[120]

Al Qaeda and bin Laden's preoccupation with income generating activities notwithstanding, even some of its most consequential operations have not proven expensive to orchestrate. Indeed, terrorist attacks themselves are not very costly to mount. It is the maintenance of the organization, the salaries paid and benefits provided to members and logistical expenses that appear to eat into a terrorist group's budget. For example, the explosive device used at the World Trade Center bomb—which was constructed out of ordinary, commercially-available materials including lawn fertilizer (urea nitrate) and diesel fuel——cost less than $400 to construct. It was nonetheless exponentially more effective: killing six persons, injuring more than a 1,000 others, gouging out a 180-ft wide crater six stories deep, and causing an estimated $550 million in both damages to the twin tower and in lost revenue to the business housed there.[121] According to the CIA, the 1998 East Africa bombings of the U.S. embassies in Nairobi and Dar-es-

---

119 Anonymous, Through Our Enemies' Eyes: Osama bin Laden, Radical Islam, and the Future of America (Dulles, VA: Brassey's, 2002), pp. 93 & 98.

120 Ibid., pp. 94, 128, 140.

121 N.R. Kleinfeld, "Legacy of Tower Explosion: Security Improved, and Lost," *New York Times*, 20 February 1993; and, Richard Bernstein, "Lingering Questions on Bombing: Powerful Device, Simple Design," *New York Times*, 14 September 1994.

Salaam, Tanzania required no more than $10,000——and succeeded in killing 301 persons and injuring 5,000 others.[122] And the 9/11 Commission estimated that Al Qaeda spent between $400,000-$500,000 to finance the 9/11 attacks.[123] Its effects, of course, on both the U.S. and global economy and the vast expenditures on security measures world-wide that have followed have of course been disproportionately immense. Bin Laden himself specifically lauded the cost-effectiveness of the 9/11 attacks in the videotaped message released just before the U.S. national elections on 29 October 2004. After citing a statement made at a conference held by the venerable London-based Royal Institute of International Affairs that Al Qaeda "spent $500,000 on the event while America, in the incident and its aftermath lost——according to the lowest estimate——more than $500 billion . . . ." He then credited the attacks with setting in motion America's current budget deficit problems, stating that this sum "has reached record astronomical numbers estimated to total more than a trillion dollars."[124]

Previous major Al Qaeda attacks also reflected an equally handsome return on investment. As the leader of a radical Egyptian jihadi terrorist group was quoted a month after the October 2000 maritime suicide attack on the *U.S.S. Cole*, a U.S. Navy destroyed anchored in Aden, Yemen, stating that operation similarly cost Al Qaeda no more than $10,000.[125] In addition to claiming the lives of 17 American sailors and wounding 39 others, it resulted in $250 million in damage to the vessel.[126]

A similarly attractive cost-effect ratio is cited by Palestinian terrorist organizations deploying suicide bombers against Israel. According to one estimate, the total cost of a typical Palestinian suicide operation, for example, is about $150.[127] Yet this modest sum yields a very attractive return: on average, suicide operations world-wide kill about four times as many persons as other kinds of terrorist attacks. In Israel the average is even higher: inflicting six times the number of deaths and roughly 26 times more casualties than other acts of terrorism.[128] Indeed, the British House of Commons Parliamentary Committee that investigated the 7

---

122 *The 9/11 Commission Report*, fn. 127, p. 498.
123 Ibid., p. 172.
124 Al Jazeera.Net, 'NEWS: Arab World——Full Transcript of bin Laden's speech,' 1 November 2004 accessed at http://Englishaljazeera.net/NR/exeres/79C6AF22-98FB-4A1C-B21F-2BC36E87F61F.htm.
125 "Militant Islamist: Attack on Cole cost 10,000 dollars." *Deutsche Presse-Agentur* (Nicosia), 12 November 2000.
126 *The 9/11 Commission Report*, pp. 212-213.
127 Nasra Hassan, 'Letter From Gaza: An Arsenal of Believers,' *The New Yorker*, 19 November 2001, p. 39.
128 RAND Terrorism Databases.

July 2005 suicide bombings of three London underground trains and a bus concluded that the attacks cost less than $8,00 to execute. This sum included the two overseas trips that the leader of the cell made as well as the second trip when he was accompanied by one of the other bombers; purchase of all the bomb making equipment; the rent on the apartment that the bombers used when constructing the bombs; hiring cars; going on a "team-building" white-water rafting trip; and, other activities.[129]

PIRA operations in the 1990s also show how relatively inexpensive, but enormously consequential, terrorist acts are to execute. The explosives used in large, (non-suicide) truck bombs, for instance, were constructed out of ordinary, commercially-available fertilizer (such as was used in the 1993 World Trade Center bombing) and were successful in devastating downtown, commercial districts both in Northern Ireland and on the mainland. In April 1992, in what was described "as the most powerful explosion in London since World War II," a PIRA bomb constructed with up to a ton of fertilizer exploded outside the Baltic Exchange building in the heart of the city's financial center, killing three persons, wounding 90 others, leaving a 12-foot wide crater and causing $1.25 billion in damage.[130] Exactly a year later, a similar bomb devastated the nearby Bishops Gate district, killing one person and injuring more than 40 others. Initial estimates put the damage at $1.5 billion.[131] Long a staple of PIRA operations, fertilizer costs on average one percent of a comparable amount of plastic explosive. Although, after adulteration, fertilizer is far less powerful than plastic explosive (i.e., Semtex explodes at about 8,000 yards a second and has a high explosive rating of 1.3; improvised explosives explode at only about 3,000 yards a yard and range between 0.25 and 0.8 in rating), it also tends to cause more damage than plastic explosives because the energy of the blast is sustained and less controlled.[132]

On the low-end of the bomb-making spectrum, during that same time period, PIRA also perfected the use of smaller bombs detonated by using

---

129 See Honourable House of Commons, *Report of the Official Account of the Bombings in London on 7th July 2005* (London: The Stationary Office, HC 1087), 11 May 2006, titled "Were They Directed From Abroad?" pp. 24-27, accessed at http://www.official-documents.co.uk/document/hc0506/hc10/1087/1087.asp.p. 23

130 William E. Schmidt, "One Dead, 40 Hurt as Blast Rips Central London," *New York Times*, 25 April 1993. See also, William E. Schmidt, "With London Still in Bomb Shock, Major Appoints His New Cabinet," *New York Times*, 12 April 1992; "Delays Seen in London," *New York Times*, 13 April 1992; Peter Rodgers, "City bomb claims may reach £1bn," *The Independent* (London), 14 April 1992; and David Connett, "IRA City bomb was fertilizer," *The Independent* (London), 28 May 1992.

131 William E. Schmidt, "One Dead, 40 Hurt as Blast Rips Central London," *New York Times*, 25 April 1993; and "Richard W. Stevenson, "I.R.A. Says It Placed Fatal Bomb: London Markets Rush to Reopen." *New York Times*, 26 April 1993.

132 Roger Highfield, "Explosion could have wrecked city centre," *Daily Telegraph* (London), 13 August 1993.

a photo-flash "slave" unit that can be triggered from a distance of up to 800 meters by a flash of light. The device, which sold at the time for between £60 and £70, is used by commercial photographers to produce simultaneous flashes during photo shoots. The PIRA bombers attach the unit to the detonating system on a bomb and then simply activate it with a commercially-available, ordinary flashgun.[133] As with the new "photo-flash" means of detonation, the sophistication of a device is often its very simplicity. In recent years, for example, the PIRA has mounted a highly effective campaign of "economic warfare" using simple incendiary devices left in Belfast and London department stores. Using a plastic cassette tape container, a miniature detonator, a timing device powered by a radio battery, a small amount of plastic explosive or explosive power, two or three capsules of lighter fuel and some paper to ensure combustion, the devices are small, highly portable, easily constructed and planted, and nearly risk-free to the bomber as the timer can usually be set for up to 12 hours. They cost less than £5 to produce[134] and have thus far caused more than $15 million in property damage.[135] The process of planting the devices is typically a one person job, but allows that person potentially to operate without detection over a wide area and thus create an impression "of a concerted attack involving a large team."[136]

Conclusion

Twenty-two years ago the inflight bombing of Air India flight 182 and the bomb explosion that occurred as baggage was being transferred at Tokyo's Narita Airport from Canadian Pacific Flight 003 to a waiting Air India flight stunned and shocked the world. The incidents demonstrated that no country is immune to terrorist violence and how easily any country and its citizens can become enmeshed without warning in local conflicts fought in distant places. The tragic loss of life both over the Irish Sea and at Narita Airport and the mostly forgotten consequences of the two bombings may at first glance seem incomparable with the death

---

133 Nicholas Watt, "IRA's 'Russian roulette' detonator," *The Times* (London), 16 March 1994; and, "Photoflash bomb threat to the public," *The Scotsman* (Edinburgh), 16 March 1994

134 Duncan Campbell, "Video Clue to IRA store blitz: Simplicity of incendiary device makes disruption easy," The Guardian (London), 24 December 1991.

135 James F. Clarity, "On Ulster Border, Grim Days for Grenadier Guards," *New York Times*, 23 February 1994.

136 Campbell, "Video Clue to IRA store blitz: Simplicity of incendiary device makes disruption easy," 24 December 1991.

toll caused by the September 11th 2001 attacks and the profound global repercussions of that fateful day. But this is not in fact the case. Any loss of life from terrorism, whatever the number, is as tragic as it is lamentable. Further, the lessons of Air India, though nearly a quarter of a century old, loom large with respect to both our current understanding of terrorism and our ongoing efforts to counter such threats.

First, with respect to the terrorism dimension, what was so shocking and stunning about Air India 182 and the Narita Airport explosion was its coordination and near simultaneity coupled with the large loss of life. Both before and since those two incidents, coordinated, simultaneous terrorist attacks only one terrorist incident——the September 11th attacks——has claimed a larger number of lives. Moreover, the same aspects of coordination and simultaneity that made the Air India and Narita Airport incidents so compelling, similarly galvanized world attention on September 11th.

Second, and hereafter, with reference to counterterrorism, the complexity of the roles and relationship of both intelligence and law enforcement in pre-empting and preventing terrorist attacks, as well as investigating and explaining them following their occurrence, remains as salient and complicated today as they were 22 years ago.

Third, the importance of both "environmental" and operational intelligence remains as clear today as it was in 1985. Detailed knowledge and understanding of both are needed if the authorities are to be able to identify and apprehend terrorists concealed within the general population or embedded within specific ethnic, religious or radical communities.

Fourth, the intersection of domestic intelligence-gathering and foreign intelligence acquisition continues to be a prominent national security concern, especially when terrorists based overseas establish networks and an infrastructure among immigrant communities or other ethnic or religious groups within a country. Issues of perceived or actual civil liberties violations due to profiling, monitoring, and surveillance have in fact only been heightened since September 11th.

Fifth, the clandestinity of terrorist cells, the difficulties of penetrating them, and the compartmented nature of terrorist operations necessitate that the authorities have the necessary (in some circumstances, extraordinary) legal powers and tools to neutralize the unique criminal threat terrorism

poses to society. The arrogation of these powers to law enforcement and intelligence and security agencies must also be overseen and monitored to prevent the perception and infringement of civil rights.

Sixth, given the globalized nature of terrorism, both today and as evidenced by the 1985 incidents, the use of highly sophisticated and technologically advanced national intelligence assets (such as signals intelligence) is critical.

Seventh, intelligence and to a growing extent law enforcement have important "patrolling" roles whereby they must have the authority and tools with which to "scan the horizon for potential threats" long before the actual commission of a terrorist act occurs, in order to acquire the knowledge necessary to pre-empt or prevent such an attack. Pre-empting and preventing terrorism thus means enabling the authorities to respond to a *potential* crime before it is committed.

Finally, the importance of examining a terrorist event that occurred nearly a quarter of a century ago cannot be minimized. It is critical not only to provide some kind of closure for the families and loved ones of the victims of that tragedy but also because it is in the best interests of a country's national security. The most fundamental expectation that citizens have of their government is that it will provide for their security and protection. Indeed, when any breakdown of this process occurs, appropriate steps must be instituted to redress the gap(s) in a country's defenses and prevent its recurrence. The value of such an investigation is clear: demonstrating to terrorists and all those who may break the law and kill and harm wantonly, that despite the passage of time, a government's determination to protect its population, defend its territory and seek to understand any past lapses and prevent any future one remains incontestable.

PROFESSOR BRUCE HOFFMAN

Professor Bruce Hoffman has been studying terrorism and insurgency for more than thirty years. He is currently a tenured professor in the Security Studies Program at Georgetown University's Edmund A. Walsh School of Foreign Service, Washington, DC. Professor Hoffman previously held the Corporate Chair in Counterterrorism and Counterinsurgency at the RAND Corporation and was also Director of RAND's Washington, D.C. Office. Professor Hoffman was adviser on counterterrorism to the Office of National Security Affairs, Coalition Provisional Authority, Baghdad, Iraq during the spring of 2004 and from 2004-2005 was an adviser on counterinsurgency to the Strategy, Plans, and Analysis Office at Multi-National Forces-Iraq Headquarters, Baghdad.

Professor Hoffman was the founding Director of the Centre for the Study of Terrorism and Political Violence at the University of St Andrews in Scotland, where he was also Reader in International Relations and Chairman of the Department of International Relations. He holds degrees in government, history, and international relations and received his doctorate from Oxford University. In November 1994, the Director of Central Intelligence awarded Professor Hoffman the United States Intelligence Community Seal Medallion, the highest level of commendation given to a non-government employee, which recognizes sustained superior performance of high value that distinctly benefits the interests and national security of the United States.

A revised and updated edition of his acclaimed 1998 book, *Inside Terrorism*, was published in May 2006 by Columbia University Press in the U.S. and S. Fischer Verlag in Germany. Foreign language versions of the first edition have been published in ten countries.

A Brief on International Terrorism

Professor Michael A. Hennessy, Ph.D.
Chair, Department of History
Royal Military College of Canada

Aim:

This brief outlines issues concerning the phenomenon of International Terrorism, its definition, dimensions and certain characteristics to aid further research.

Introduction:

On the night of 23 June 1985 Air India Flight 182 fell in pieces into the ocean off the West Coast of the Republic of Ireland. All 329 people aboard were lost. Preliminary analysis and subsequent investigation conclude the flight was destroyed by a small explosive device presumably placed in the aircraft at its port of departure in Canada. Evidence and speculation since this event suggests the bombing was carried out by elements of a religious-nationalist group of Canadian and Indian Sikhs engaged in an armed struggle to form the separate Sikh controlled state of Khalistan. This report does not address the validity of those claims, rather, it aims to contextualize the methods adopted during this reported armed struggle with the wider discussion of the phenomenon of 'international terrorism' which plagues the world today.

"Terrorism" origins of a construct

"Terrorism" and 'terrorist' remain highly emotive terms and in some senses are continually evolving in their meaning and usage. In that sense they are living terms, concepts and mental constructs. The use of the term "terrorist" to refer to politically motivated violence goes back to revolutionary France. The term gained currency when after 1792, the Jacobins came to power and initiated what became *La Terror*, the Reign of Terror. In 1795 the British observer Sir Edmund Burke popularized the term 'terrorist' and 'terrorism' as pejoratives against those French revolutionaries that espoused *the purposeful effusion of blood as both a purifying and defensive ingredient of their revolution.*

Gradually the term "terrorism" came to be applied to violent revolutionary activity in general. Through the late 19th Century the term more and more became associated with violent attacks against the government or dominant social order with both Irish resistance to British control and Russian anti-Czarist campaigns being condemned under the title 'terrorist'—an epithet that Russian revolutionaries adopted for themselves from time to time.[1]

---

1 See, Lindsay Clutterbuck, "The progenitors of Terrorism: Russian Revolutionaries or Extreme Irish Republicans," *Terrorism and Political Violence,* 16:1 (Spring 2004), pp. 154-181.

Burke's first pejorative usage of the term terrorist remains important. It remains a commonplace that 'one man's terrorist is another man's freedom fighter.'[2] As an observation it is irrefutable –those who embark on a campaign of violence, generally described as terrorism, rationalize their activities as justified and moral, however 'illegal'. This point of moral certainty will be returned to.

By the mid-20th century, terrorism was becoming associated more with movements of national liberation than with radical groups, and the word was starting to acquire its universal stigma. Bruce Hoffman attributes the birth of 'international terrorism' to the increase in the hijacking of international flights instigated by the PLO[3] in the late 1960s. This period saw a spate of airline hijackings and culminated spectacularly with the attack by "Black September"[4] on the Israeli athletes' dormitories at the Munich Olympic Games in 1972. These activities were characterized by planned and organized violence against those generally regarded as innocent or non-combatants. Further, these forms of attack were generally part of a systematic or sustained campaign of violence and agitation that is different from more spontaneous or expressive acts like riots or organized mass protests. Terrorism then is a tactic that employs violence to alter the political landscape or process. Contemporary examples of 'terrorist movements' illustrate there are many motives behind such activity. Motives range from ethnic, religious, economic, political and international issues, but whatever the motive, terrorism has been employed as a tool in many countries and between nations to compel political or social change.

Not all terrorism may be conceived within so instrumental a purpose. Since the late 1980s an increasing amount of literature on terrorism has identified a growing trend that some terrorism has taken on a new dimension that is far less instrumental and more nihilistic, hence harkening back to the radicalism of the anarchist movement of the 19th century – but with an important distinction, whereas the nihilist/anarchists of the 19th century focused their attacks against members or representatives of the respective political/social regimes they attacked, the later period has been marked by the rise of efforts to cause mass casualties. Walter Laqueur identified this trend in his work on 'post modern' terrorism, and

---

2 Kennedy, Robert. "Is One Person's Terrorist Another's Freedom Fighter? Western & Islamic Approaches to "Just War" Compared." In *Terrorism and Political Violence* Vol. 11, No. 1, (Spring 1999): 1-21.

3 Palestinian Liberation Organization.

4 Popular Front for the Liberation of Palestine.

he and Bruce Hoffman and others have remarked on what they term the 'new terrorism'—a distinction that pre-dates the events of September 11th, 2001. This 'new terrorism' is marked by a more totalistic ideology, generally religious, it does not rely on a sovereign state for support, and has little or no desire to constrain its violence which in some instances has verged on the apocalyptic.[5]

This background is essential for contextualizing the various definitions that are available.

Terrorism Defined

There remains no universally accepted definition of international terrorism. The United Nations General Assembly continues to argue over an agreed definition, but there are many national acts of legislation and increasing international agreements that move toward defining the term. Many jurisdictions already have laws that cover the range of violent phenomenon associated with 'terrorism' e.g. murder, destruction of property, inflicting serious injury, intimidation, threats of violence, hijacking etc. None of these activities, however, fully capture the range of activities that 'terrorists' partake in and that is also not to raise the issue of 'state sponsored' terrorism.[6]

Although the terms terrorist and terrorism are today in wide common usage and while there are government regulations and international agreements for the control of terrorist activities there is in domestic law only a small set of statutory definitions. The 1999 International Convention for the Suppression of Financing of Terrorism provides one of the most consensual definitions by making it a crime to collect or provide funds gathered *for or with the intent of supporting the killing or injuring of civilians*

---

5 See Laqueur, "Postmodern Terrorism: New Rules for an Old Game," *Foreign Affairs*, (sept/Oct.1996), contrast with his later work and that by Bruce Hoffman, et al, see discussion in "America and the New Terrorism: an Exchange," *Survival*, 42:2 (June 2000), pp. 156-172. and Steven Simon and Daniel Benjamin, "America and the new terrorism," *Survival* 42:1 (Spring 2000), pp. 59-75. On the apocalyptic see Robert J. Lifton, *Destroying the World to Save it. Aum Shinrikyo, Apocalyptic Violence, and the New Global ____Terrorism*, (Henry Holt: New York, 1999, and 2000.).

6 Terrorism has also been associated with forms of state versus state violence both overt and covert. Hence the term 'state sponsored terrorism' has come into common usage. As adjunct to a wider conventional war, or as part of a war by proxy many nation states have employed tactics and methods more commonly associated with terrorism. This later feature of the international system is not explored further in this paper except to note that some have argued the possibility that the Air India bombings were conducted by the Indian state itself as a measure to de-legitimize the choice of violence by a group of Sikh nationalists ex-patriots resident in Canada—a type of phenomenon not unknown to history.

where the purpose is to intimidate a population or coerce a government.[7]
It might well be asked what constitutes a 'civilian', but the key points here are intimidation and coercion by violence or the threat of violence and the acts can be likened to subversion by violence.

An example of a quasi legal definition of terrorism is that used by the US Federal Bureau of Investigation (FBI) which reads " the unlawful use of force against persons or property to intimidate or coerce a government, the civilian population or any segment thereof, in the furtherance of political or social objectives".

Like many similar definitions this one includes three elements:
(1) Terrorist activities are illegal and involve the use of force.
(2) The actions are intended to intimidate or coerce.
(3) The actions are committed in support of political or social objectives.

The US State Department's definition reads: "Premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, usually intended to influence an audience."

"International" terrorism is defined as "terrorism involving citizens or the territory of more than one country".

The above American definitions are notable in that they exclude overt acts of violence and intimidation by a state.

The Canadian statute definition is found in the Criminal Code and is reproduced here at some length.

The Canadian Criminal Code reads as follows:
"terrorist activity" means

(a) an act or omission that is committed in or outside Canada and that, if committed in Canada, is one of the following offences:

---

7 See, http://untreaty.un.org/English/terrorism.asp. And CRS Report RL 33600 R F. Perl, "International Terrorism: Threat, Policy and Response," (Washington, 9 Aug. 2006), pp. 29-30. See also CRS Report RS21021, by Elizabeth Martin, "Terrorism and Related Terms in Statute and Regulation: Selected Language." On the recommended UN definition see, UN, *A More Secure World: Our Shared Responsibility*. Report of the Secretary General's High-level Panel on Threats, Challenges and Change, New York, 2004), esp. pp. 51-52.

(i) the offences referred to in subsection 7(2) that implement the Convention for the Suppression of Unlawful Seizure of Aircraft, signed at The Hague on December 16, 1970,

(ii) the offences referred to in subsection 7(2) that implement the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on September 23, 1971,

(iii) the offences referred to in subsection 7(3) that implement the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on December 14, 1973,

(iv) the offences referred to in subsection 7(3.1) that implement the International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on December 17, 1979,

(v) the offences referred to in subsection 7(3.4) or (3.6) that implement the Convention on the Physical Protection of Nuclear Material, done at Vienna and New York on March 3, 1980,

(vi) the offences referred to in subsection 7(2) that implement the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, signed at Montreal on February 24, 1988,

(vii) the offences referred to in subsection 7(2.1) that implement the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on March 10, 1988,

(viii) the offences referred to in subsection 7(2.1) or (2.2) that implement the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf, done at Rome on March 10, 1988,

(ix) the offences referred to in subsection 7(3.72) that implement the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on December 15, 1997, and

(x) the offences referred to in subsection 7(3.73) that implement the International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations on December 9, 1999, or

(b) an act or omission, in or outside Canada,

(i) that is committed

(A) in whole or in part for a political, religious or ideological purpose, objective or cause, and

(B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and

(ii) that intentionally

(A) causes death or serious bodily harm to a person by the use of violence,

(B) endangers a person's life,

(C) causes a serious risk to the health or safety of the public or any segment of the public,

(D) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or

(E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C),

and includes a conspiracy, attempt or threat to commit any such act or omission, or being an accessory after the fact or counselling in relation to any such act or omission, but, for greater certainty, does not include an act or omission that is committed during an armed conflict and that, at the time and in the place of its commission, is in accordance with customary international law or conventional international law applicable to the conflict, or the activities undertaken by military forces of a state in the exercise of their official duties, to the extent that those activities are governed by other rules of international law.
"Terrorist Group" means

(a) an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity, or

(b) a listed entity,

and includes an association of such entities.

For greater certainty

(1.1) For greater certainty, the expression of a political, religious or ideological thought, belief or opinion does not come within paragraph (b) of the definition "terrorist activity" in subsection (1) unless it constitutes an act or omission that satisfies the criteria of that paragraph.[8]

All legal definitions, including Canada's tend to agree on these points but it remains difficult to frame civil laws that fully capture and then proscribe the scope of activities that 'terrorist' organizations partake in because larger terrorist organizations have many activities and attract many adherents who are not directly involved in conducting violence or similar illegal activity save formal or 'informal' membership in what might be declared an illegal organization. Civil law may not overcome this difficulty and may not be the appropriate tool for dealing with such forms of armed struggle and the historical record of special status laws is ambiguous.

---

8 Criminal Code of Canada, accessed http://justice.gc.ca.

Causes

International terrorism waged by non-state actors has been attributed to a number of causes—political, social, economic and psychological. In many instances these terrorist actions cannot be decoupled from larger or more regular armed struggles, ongoing guerrilla warfare, insurrectionary acts, rebellion, national liberation struggles or other uses of violence in pursuit of political or social change. Terrorism is regarded in many circles as a legitimate response to forms of state repression (real or imagined) and has accompanied the activities of the IRA in the United Kingdom, the Tamil Tigers' struggles in Sri Lanka or the Basque ETA struggle in north west Spain. As well, minorities in divided societies, both secessionist or irredentist, such as the Sikh Khalsa in India, have made recourse to the tactic of employing terror.

Unlike state-sponsored terrorism that can be rationalized through some calculus of *raison d'état*, non-state terrorism raises unique questions about who participates in such activity. The rise of 'professional terrorists' however is not unique to this age, certainly the anti-Czarist movements of the 19th century championed the cult of self sacrifice of the dedicated revolutionary embarked on a campaign of violent struggle.[9]

Although not a phenomenon unique to our age, difficult questions remain about who participates. Questions are raised about the socialization process of those attracted to voluntarily participating in such activities as mass murder. The psychological literature offers diverse interpretations but it can be said there is little support for the basic proposition that those who embark on such activities are psychologically deficient, crazy or particularly sociopathological, psychotic or otherwise clinically insane, anti-social or suffering from other major personality disorders.[10]

More fruitful than efforts at individual terrorist profiling is analysis of group behavior, particularly the process by which individuals bond within a group that progresses them toward the normalization of violence. The work by Janis on 'Groupthink' is particularly fruitful in explaining the process and pathology of group behavior giving delusions of

---

9 See Laqueur, *A History of Terrorism*, *passim*.

10 See, John Horgan, *The Psychology of Terrorism* (2006), and Rex . Hudson, "The Sociology and Psychology of Terrorism: Who Becomes and Terrorist and Why?" Federal Research Division US Library of Congress, 1999.

invulnerability, re-enforcing group morality, yielding a one dimensional view of what is construed to be the 'enemy' and also acting to limit in-group challenges to the groups' shared beliefs—this point will be taken up when discussing terrorism as a communications strategy.[11] The nature of these group networks is explored in some detail in the work by Marc Sageman (a psychologist), in his *Understanding Terror Networks*.[12] While each group undoubtedly has unique traits Sageman's work suggests that any effort at profiling must consider group relationships and dynamics, rather than purely individual profiles. This form of *link analysis* will remain problematic for intelligence agencies and the courts because it runs so close to the problems of guilt by association.

The In-group, Out-group characteristic of terrorist organizations is very important. First of all it helps to de-humanize potential targets by reinforcing stereotypes of the 'other.'[13] While the 'group' shares a construct of what is right and just about their cause and actions they have also constructed an enemy and in many instances the more abstract or ideal the enemy the more extreme the violence—but that is also characteristic of other forms of warfare.[14]

While the group dynamics and the contours of the motivating ideology are important elements to identify they may not explain the choice or forms of violence. Efforts to explain the choice of violence fall into two broad camps. Actions against that 'enemy' can be viewed as *instrumental violence*, that is violence aimed at having the enemy change its ways. A number of scholars argue terrorism can be understood in that sense as highly rational, indeed the outcome of strategic choice—I'll explore terrorism as a strategy momentarily.

Other experts argue the violence may not have any instrumentality except as a means of reinforcing the group's identity, the acts justify and reinforce the group's identity and existence.[15]

---

11 I. Janis, *Victims of Groupthink*, (Boston: H. Miflin, 1972), Gerald Post, "Terrorist psycho-logic: Terrorist behavior as a product of psychological forces," in Walter Reich, ed. *Origins of Terrorism. Psychologies, Ideologies, Theologies, States of Mind*, (Woodrow Wilson Center Press, Washington, D.C., 1998), see also Horgan and Hudson above.

12 Marc Sageman, *Understanding Terror Networks*, (University of Pennsylvania Press, Philadelphia, 2004).

13 Terrorism is not unique in this regard so for example the many cases explored in Robert S. Wistrich, ed. Demonizing the Other. *Antisemitism, Racism, and Xnophobia*, (Harwood Academic Publishers, 1999).

14 On the growth of more extreme views during a terror campaign see Michel Wieviorka, *The Making of Terrorism*, D.G. White trans., (Chicago, 1988). For a narrative of how revolutionary groups maintain internal loyalty see the comparative discussion in Jon Lee Anderson, *Guerrillas. Journeys in the Insurgent World*, (London: Penquin, 1992, 2004.)

15 See the divergent views of M. Crenshaw and J. Post in Reich, *Origins of Terrorism*.

Terrorism as a Strategy

Terrorism as an instrumental and rational act can be considered as framed within a strategic concept not unlike that associated with more conventional forms of warfare—in that sense it can be seen as a means of asymmetrical war, but is primarily a choice of the side weakest in conventional military strength. In conventional warfare the leadership sets goals and designs a plan of campaign to achieve those goals. Ways, means and ends are aligned and steps are taken to bring sufficient means together to accomplish the higher ends of policy—at least that is the rational model. Terrorism, however, is a tactic adopted by forces that generally do not possess more or sufficient means of waging conventional warfare thus individual terrorist acts may be the only form of violence open to them and they may or may not be conceived within a wider or general campaign plan. The weaker force makes a virtue of its weakness, but has also chosen not to employ other less violent means of 'resistance'. Indeed its higher strategy may simply be to wage sporadic acts of terror, thus reducing 'terrorism' to a strategy of tactics in which each episode of terror is a full round in a series of games between the established order (targeted government) and the terrorists. This might be aimed at forcing an overreaction of the security forces, or as a means of gaining support, or demonstrating resolve or motivating existing followers...or something else. Forces might well feel driven to such tactics because they are inferior in the face of their adversary's conventional military strength. The materially weaker side then will frame the terror campaign as part of a protracted warfare struggle. Modern mass democracies are generally not well prepared in law or otherwise to deal with an internal adversary bent on fighting a *protracted war.*

The basic tactics open to the weaker force are generally well known: theft, intimidation, propaganda, assassination, hostage taking, or kidnapping, hijacking, and bombing. To employ any of these methods certain instrumentalities are necessary. The terrorist organization needs people, and organization, access to the appropriate technology and the financial resources to acquire it, and probably an animating ideology. For a campaign to grow the terrorist group must have a method of growing its organization—although there are examples like the Canadian group Direct Action which did not plan for formal growth.[16] Every group that can

---

16 Ann Hansen, *Direct Action. Memoirs of an Urban Guerrilla*, (Between the Lines: AK Press, 2001, 2002.). This account by a Canadian raised domestic terrorist could also serve as a basic training manual for one so inclined. It is also revealing of her path to radicalization.

be examined in any detail will reveal a formal structure (even in the case of 'leaderless resistance'[17]) with its own dynamics but generally aimed at addressing similar types of issues, such as access to people, money, training, planning, intelligence, propaganda, recruiting and resources essential for the conduct of violent activities.

Some organizations have embarked on this path as a last resort, others as the first resort. A partial answer as to why the path of violence is chosen can generally be found in how various groups articulate their mobilizing ideology—be it religious, social, ethnic or some other group identity. These motives are often revealed in the forms of propaganda employed by groups.

Terror as a Communications Strategy

Nineteenth century anarchist writings referred to their attacks as "propaganda of the deed." Modern terrorism can also be seen in that light. Terror as an instrumental policy can be an end in itself, to simply demonstrate an ability. Equally it could be aimed at contributing to a conscious effort to wage a protracted struggle. It can be aimed at changing an immediate condition or policy. It can be aimed at bringing political change onto the political agenda. Some groups have articulated policies that aim at creating revolutionary conditions by exciting the masses or imaginations of blocs of the population to fuel the call for change. It can be aimed at motivating the target government to embark on a campaign of ruthless repression thus destroying the state's legitimacy or costing it mass appeal. It can be aimed at forcing the government to seek compromise. Or it may be a campaign of single deeds—the blows are the message.

Terrorism can be seen then to have multiple audiences and various acts may not be tailored to address them all. Its methods however clearly aim at targeting a few, as Martha Crenshaw has put it, 'in a way that claims the attention of the many. Thus a lack of proportion between resources deployed and effects created, between the material power of actors and the fear their actions generate is typical."[18] Like other forms of

---

17 This term is not well used in the literature, but it describes well the type of organization the second stage Al Qaida campaign has taken. The term comes from American based right wing paramilitary writings. See, Lewis Beam, "Leaderless Resistance," (1992), at www.louisbeam.com/leaderless.htm

18 Crenshaw in Reich, p. 4.

propaganda the message may target multiple audiences and may remain rather ambiguous. While instilling fear, the actions of the terrorists may be portrayed as heroic, noble and full of self sacrifice—that message will resonate with some, but not others. The actions might be geared to fostering compromise, or preventing it, towards instilling confidence amongst the terrorist's affinity group, while destroying confidence among the target community. Further, the action's rationale might be found in mixed motives, wherein the motive ideology is not clearly bounded and wherein contradictions within the terrorist community are not fully resolved. But the search for why such actions are conducted may have to look no further than the explanation that violence is an end in itself—that is the logic of the concept of 'propaganda of the deed'.[19]

In the case of the Air India bombing, for instance, one might search for a rational cause for killing over three hundred innocents. It could be explained as a blow against the Indian government as punishment for the alleged oppression of the Sikh community but it equally could have been motivated as an act to build group cohesion, identity and as a means of demonstrating purely to like minded individuals the reach or potency of the group involved. I.E. the external audience was not the target. Equally, the bombing can be seen merely as an effort of retributive 'justice'.[20]

Threat Analysis

Such ambiguity makes generalizing and the framing of predictive models very difficult. Disentangling the motive may prove impossible. This ambiguity greatly complicates the task of threat analysis and assessment—methodologies for which there are no agreed international standards or methods. While the Canadian Integrated Threat Assessment Centre has developed its own methods these are not discussed in detail in the open literature—but such 'methods' are not likely to have overcome the various problems associated with all methods.[21] Whereas criminal law aims at deterring and then punishing, the state's responsibility for maintaining order and security may require a greater range of activities. Intelligence and security operations are aimed at deterring but also

---

19 For instance it has been argued that there is a Quranic concept of war that states that terror is not a means of imposing decision upon the enemy; it is the decision we wish to impose upon him, cited in Yossef Bodansky, *Bin Laden: The Man Who Declared War on America*, (Roseville, CA, 1999), p.xv.

20 For a discussion of the latter see, Stéphane Leman-Langlois. and Jean-Paul Brodeur, "Terrorism Old and New: Counterterrorism in Canada," *Police Practice and Research*, v.6.n2. (May 2005). pp. 121-140.

21 On a survey of methods see, US General Accounting Office report, 'Combating Terrorism. How Five Foreign Countries Are Organized to Combat Terrorism,' GAO/NSAID-00-85, April 2000.

preventing and protecting from possible acts. Building a criminal case after the fact is only part of the intelligence problem. Monitoring groups of interest depends often on only fragmentary information from which must be built an assessment of intentions, and capabilities. Intelligence sharing, systematic link analysis, surveillance and other forms of collection and analysis are confounded by not well bounded problems and the difficulties of discovering both real criminal intention and finding manifest capability, both of which a potential adversary will attempt to shield from detection. There is no simple, normative solution.[22]

22 See, "Threat Levels: The System to Assess the Threat from International Terrorism," (UK Home Office, July 2006.)

Dr. Michael A. Hennessy is a Professor of History and War Studies at the Royal Military College of Canada, Kingston, Chair of the Department of History and Dean of Continuing Studies. He is the former Deputy Project Director of the Canadian Forces Leadership Institute, and remains a Research Fellow of the Institute. Dr. Hennessy served as the founding project director and editor of the *Canadian Military Journal/Revue militaire canadienne.* He remains a member of the editorial board of CMJ, and is a member of the editorial boards of the *Canadian Army Journal, the Canadian Historical Association journal*, the journal *Defence Studies, the Journal of the Joint Services Command and Staff College* (UK). He served as a member of the joint Chief Research & Development-DG Strategic Plans Operational Working Group on the Revolution in Military Affairs (RMA) that outlined Canada's response to the RMA and subsequent publication of *Strategy 2020.* As well, he has worked with elements of the naval staff and air staff on their basic doctrinal documents such as *Leadmark* and *CF Aerospace Doctrine.* He has also been the Chief of Land Staff's representative on the ABCA Historical Data Analysis sub-committee.

He is a member of the International Institute of Strategic Studies and a representative to the Partnership For Peace Working Group on Terrorism and the Royal Canadian Mounted Policy Criminal Intelligence Product Review Board. His teaching fields include war technology, intelligence, foreign policy, naval policy and low intensity conflict.

His scholarly articles range from Canadian naval and maritime history, intelligence, strategy during the Vietnam War, Canadian foreign and defence policy and special operations forces. His publications include *Strategy In Vietnam: The Marines and Revolutionary War in I Corps, 1965-1971*, (Praeger, 1997), and "Operation Assurance: Planning a multinational operation for Rwanda/Zaire," *Canadian Military Journal* (Spring 2001), and with B.J.C. McKercher, *The Operational Art: Developments in the Theory of War*, (Praeger, 1996), and *War in the Twentieth Century. Reflections at Century's End*, (Praeger, 2003).

In 2001 he received CDS Commendation for his work on the CFLI and *Canadian Military Journal.*

Context is Everything: The Air India Bombing, 9/11 and the Limits of Analogy

Peter M. Archambault, PhD[1]

1 Biography attached.

Introduction

In the field of strategic analysis, it is often said that context is everything. We can be guided by this axiom when assessing the actions of governments executing their national security responsibilities, specifically when considering the context of the particular terrorist incident which gave rise to this inquiry: the bombing of Air India Flight 182 in 1985, and the Government of Canada's response to it. It is important to examine the extent to which any analysis of this context can be considered relevant to the security environment of more than a quarter of a century later. What are the defining features of the security environment that form the context from which present-day policies, practices and legislation are derived, and which are linked to Canada's security circumstances and needs? What can be said of the future? We need to be able to predict and assess future threats to national security, in order to tailor our ability to respond accordingly.

National security policies and practices are not developed in a vacuum, nor do they remain static. At any given time, governments are simultaneously assessing emerging threats, crafting strategies to address them, and enacting policies designed to ensure the defence and security of the nation. National security demands a variety of capabilities, substantial resources and a legal system that provides for extraordinary powers alongside systematic checks and balances (oversight), all of which must be integrated not only with other elements of government, but also with comparable systems in neighbouring and allied countries and our various security partners around the world. Thus, while the inspiration for the Inquiry and its principal areas of emphasis lie with the bombing of Air India Flight 182 in 1985, its recommendations will be oriented toward current and future considerations of how Canada copes, and will cope, with terrorism as a significant and growing threat to Canada's national security. This paper presents no new evidence to the Inquiry; rather, it examines the context of the evidence and proposes a conceptual framework within which the Commissioner can assess the evidence presented to him in regard to specific points contained in the Terms of Reference.[2] In so doing, it is suggested that the significance of terrorism within today's security environment is fundamentally different from that of the mid-1980s and, consequently, while there are many valuable lessons to be learned – and that have been learned -- from the Air India bombing, they should be viewed with this different context in mind.

---

2 See Appendix A.

Placing the Event: Then and Now

Telling the story of the Air India bombing and the subsequent investigation and trial is important in and of itself, not only for the families of the victims who for years have pressed for answers, but also for those engaged in studying the evils of terrorism – in all its myriad forms – and working to counter its usually devastating impact. However, the mandate of this Inquiry extends beyond establishing the facts related to the incident itself. There are expectations that lessons that may be identified and applied in the future. Speaking in Toronto at the unveiling of a memorial to the Air India victims in June 2007, Prime Minister Stephen Harper (who struck the Inquiry in May 2006) noted that one important step has already been taken in that regard: the country recognizes the "tragedy as a Canadian event." Harper went further, stating that the "real contribution of Justice Major's ultimate report [will be] advising the government and government agencies on what needs to be done to ensure that this kind of event is never repeated."[3]

This entirely appropriate and welcome guidance does raise some perplexing questions, especially for the purposes of this Inquiry.

i. What "kind" of event was it? It was certainly a terrorist event. It was certainly a violent event. It was certainly a devastating event. It most certainly was a Canadian event: the attacks were planned and executed in Canada, and most of the victims were Canadian. However, are these commonplace characterizations sufficient to allow policy-makers to draw useful conclusions about the "kind" of event the Air India bombing represents? For that matter, can anyone really guarantee that such a tragically successful attack will never again occur?

ii. Furthermore, by "event" do we mean the planning of the bombing, the bombing itself or the failure to convict its perpetrators? If so, surely it is impossible to guarantee convictions in a criminal trial.

iii. Finally, and most importantly, how informative is the Air India narrative in helping us to understand the threat of terrorism today as characterized by the attacks of 9/11?

---

3 Kim Bolan, "9/11 'Gave Life' to Scope of Air India Tragedy", June 23, 2007 (Electronic Edition – *National Post*)

In many ways, Air India exemplified the so-called "new terrorism" of increased lethality as differentiated from the traditional type of terrorism associated with left-wing or separatist movements. At the operational level, Air India/Narita and 9/11 were similar, in the sense that they both featured a complex attack, the targeting of civilians and the use of aircraft to carry out the plots.

In hindsight, it is also easy to argue that both were examples of an "intelligence failure." Much has been made of the 9/11 Commission's characterizations of the warnings leading up to 9/11, namely that "the system was blinking red," and it may be plausible to suggest that the same situation faced Canadian officials before June 1985. Furthermore, it may be tempting to echo the 9/11 Commission's judgement that, in failing to stop the attacks, the US intelligence community's "most important failure was one of imagination." Presumably, more imagination would have allowed analysts to conceive of terrorists using aircraft, and perhaps even to guard better against a surprise attack. The Commission suggested that the "institutionalization" of imagination would have helped the "unwieldy" US government to understand and appreciate the looming threat.[4]

It could be argued that the same hindrances affected the ability of Canadian officials to understand and appreciate the threat posed by Sikh terrorists in the early to mid-1980s. This point has been made in the Canadian media, with some journalists claiming, for instance, "...the worst terrorist attack in Canadian history might have been averted if clear warnings, repeated over several months, had been heeded."[5] In terms of thinking about the attacks themselves, and our ability after the fact to construct a narrative leading to them that might run like a slow-motion video, it might be tempting to interpret these arguments in such a way as to conclude that the Air India bombing was "Canada's 9/11." As tempting as it might be, that would be a false analogy.

It is not the purpose of this paper to recount or question the facts about the pre-bombing period, the bombing itself, or the investigation and criminal trial as brought forward during the Commission's hearings. It is, however, important to warn against the temptation to interpret the innumerable steps taken and decisions made, both by the perpetrators and government officials, as having been linear and unambiguous at

---

4 U.S. *The 9/11 Commission Report*. 585 pages. National Commission on Terrorist Attack Upon the U.S., 2004 pp. 344-348.

5 Macqueen, Ken and Geddes, John. "Air India: After 22 Years, Now's the Time for Truth," *Macleans*, May 28, 2007. pp. 1-7.

every step of the way. It should also be borne in mind that attributing successful terrorist attacks to failures of imagination and intelligence is also of questionable value. There is no way to anticipate or prepare to counter every conceivable threat, and overdoing this type of analysis tends to shift the responsibility for terrorist attacks away from the terrorists themselves.

Take, for instance, the bungled car bomb attacks in Glasgow and London in June 2007. Mass casualties seem only to have been avoided through a mix of good fortune on the part of the authorities, and incompetence on the part of the terrorists.[6] But the perpetrators were still the cause of the event, bungled or not. Is there still any use to attributing the events to intelligence failure or lack of investigative imagination? Would there not have been a much louder outcry to this effect if the attacks had been fully successful? While good intelligence is essential in staying one step ahead of terrorists and avoiding both strategic and tactical surprise, no intelligence agency is omniscient.[7] And the task is enormous. Consider, for instance, that in London in November 2006, only eight months before these incidents took place, the Director General of the Security Service (MI5) gave a public speech in London outlining the breadth of the terrorist threat facing that country: "... my officers and the police are working to contend with some 200 groupings or networks, totalling over 1600 identified individuals (and there will be many we don't know) who are actively engaged in plotting, or facilitating, terrorist acts here and overseas.[8]

It is wise to look at lessons learned from past mistakes, and public airings of those mistakes are a vital part of the democratic process. Democracies that value freedoms as well as the rule of law are constantly engaged in striking a balance between the two, but, in spite of this, permanent security and safety will always be illusive.

Yet, the concept of "intelligence failure" implies the opposite – that a system short of perfection is blameworthy. This view is flawed in that it fails to account for some stark facts based on a simple premise: "the enemy always has a vote." Those defending against terrorists try to avoid

---

6 Neil Ellis, "Failed Terrorist Attacks Are Still Terrorist Attacks," Royal United Services Institute for Defence and Security Studies, *Commentary*, July 2007.

7 Stephen Marrin, "Preventing Intelligence Failures by Learning From the Past," in *International Journal of Intelligence and CounterIntelligence*," vol. 17, 2004.

8 Speech by the Director General of the Security Service, Dame Eliza Manningham-Buller, given at Queen Mary's College, London, 9 November 2006 (http://www.mi5.gov.uk/output Page374.htm) accessed 5 June 2007.

being surprised, while terrorists are doing everything in their power to achieve surprise. Terrorists are adversaries with objectives of their own, and it is foolhardy and condescending to assume that we will always have the upper hand and the advantage. One of the better-known adages of the decades-old police battle against terrorists is that governments have to be lucky all of the time, while terrorists only have to be lucky once. A more complete formulation of this principle might recognize that an "intelligence failure" at our end is equally an "operational success" for the enemy. That is not to suggest that "failures" never occur, or that hindsight has no value. The fact that the July 2005 London Bombings ("7/7") occurred just two months after that country's Joint Terrorism Assessment Centre (JTAC) had lowered the threat level seems to welcome charges of "intelligence failure," but how do we differentiate between failures of intelligence and failures of policy, such as allocation of resources to the intelligence agency? If, as some have argued, MI5's strained resources contributed to its inability to effectively track and deter the 7/7 perpetrators, is that indicative of an "intelligence failure," "policy failure" or a combination of both?[9] Or, as we remember that the enemy always has a vote, should we think of 7/7 as another Al Qaedist success in their war against the West?[10]

So, in the sense that they were both terrorist "successes" the Air India bombing and 9/11 -- the latter occurring almost four years before the London bombings -- and in that respect similar. However, we should not extend that similarity and confuse the strategic significance of AI 182/ Narita with that of 9/11 within their respective strategic contexts. The political goals were in vastly different, as was the impact on Canada. Sikh terrorists might have had as their objective to do harm to India and destroy Government of India assets in furtherance of their cause, but there is no indication that they were deliberately targeting Canada or its domestic or international policies. The Air India bombing was not aimed at Ottawa; it was part of the reaction to the battle of Amritsar in 1984. Sikh militancy was and remains rooted in Indian politics and the quest for a future Sikh homeland.[11] This is akin to the roots of "traditional" terrorist groups, such as the Irish Republican Army (IRA), the Basque separatists (ETA), or the Kurdish Workers' Party (PKK), for whom terrorism is aimed

---

9 Mark Phythian, "Intelligence, Policy-Making and the 7 July 2005 London Bombings," *Crime, Law and Social Change* (2005) 44: pp. 361-385.

10 The term "Al Qaedists" is used herein to refer both to Al Qaeda and those who adhere to the ideological movements it has inspired, which may act autonomously of Al Qaeda command and control.

11 While terrorists might not have targeted Canada *per se*, its citizens were treated as pawns in their fight against India.

at achieving limited, irredentist objectives, even though funding and logistical support might come from abroad.

At the time of the Air India bombing in 1985, the strategic enemy we faced was the nuclear-armed Soviet Union. Understandably, in the Cold War context of 1985, Canadian officials did not consider terrorism to be as significant as they do today, largely because the potential consequences differed so greatly. Canada, like its Western allies, saw Soviet policies and capabilities as an existential threat to the survival of the western democracies, and high-level policymaking was focussed on devising strategies and developing capabilities to deter and defeat it. Ultimately, this focus was borne out; the Western allies won the long Cold War.

But that war was not just about power, it was about ideology. The Soviet Union and the United States, along with the former's satellites (Warsaw Pact) and the latter's allies (NATO), represented two distinct and fundamentally incompatible world views – one collectivist and authoritarian, and the other free and democratic. For Canada, the Soviet Union was the enemy and communism was an implacable, proselytizing ideology to be resisted. The enemy had proven both its capability and its intent, through aggressive action taken soon after the victory over the Axis in 1945. The Soviet subjugation of Eastern Europe, the "Iron Curtain", the Berlin blockade, the Soviet nuclear test, Korea – these events could be, and were, taken as prima facie evidence of Moscow's hostile intent. Western governments faced the task of framing and countering that state-based threat to their own security and that of their allies. The challenge of doing so was made easier, of course, by the context: the Second World War clearly exhibited the hazards posed by aggressive totalitarian regimes possessing highly capable armed forces.

We have little background and context to prepare us for the long struggle embarked upon after 9/11 but, in many ways, that day marked a new type of threat, in a new kind of security environment. In many ways, the threat is like that posed by the Soviet Union: ideological and long-term. It is important to set it within our new security environment to demonstrate the limited relevance of the Air India narrative to today's context.

Threats and Challenges: The Politics of Focus

Since the fall of the Berlin Wall, no peer competitor to the United States has emerged, and the Manichaean struggle of the Cold War no longer

provides the context in which threats are framed. As a result, it has become commonplace to argue that thinking about security should expand beyond "traditional" state-based military assessments. From this perspective, those who work in the security and defence fields should focus not just on existential threats posed by enemies, but also on an ever-expanding array of trends and challenges that might affect international security, but that pose no direct threat to the countries for whose governments they work. Inherent in this approach is the assumption that the "national security state" is increasingly irrelevant and is gradually giving way to globalization and (at least) three general changes in the international security environment that diminish the effectiveness of individual states.

i. First, the likelihood of high intensity warfare between capable states has given way to low intensity conflict within states and between less capable states.

ii. Second, more powerful states face the spectre of "post-industrial warfare," wherein individuals and small groups, driven by ideological fury, can hack computer networks, disrupt economies, commit acts of terrorism or harass professional militaries engaged in operations; and

iii. Third, transnational threats, such as environmental degradation, climate change, drug trafficking, poverty and the spread of infectious disease may be beyond the capability of individual states to handle.

The immediate implication of this "globalized" approach to threat assessment, released from the constraint of identifying threats to national interests, is that it makes for a very long list of things to worry about. Reporting in 2004, the UN High Level Panel on Threats, Challenges and Change insisted that this entire list of changes in the international security environment actually consists of "threats," which it defined thus: "Any event or process that leads to large-scale death or lessening of life chances and undermines States as the basic unit of the international system is a threat to international security." Under this definition, the Panel argued that there are "six clusters of threats with which the world must be concerned now and in the decades ahead:

i. Economic and social threats, including poverty, infectious diseases and environmental degradation;

ii. Inter-State conflict;

iii. Internal conflict, including civil war, genocide and other large-scale atrocities;

iv. Nuclear, radiological, chemical and biological weapons;
v. Terrorism; and

vi. Transnational organized crime.[12]

Most lists purporting to address the nature of the "threats" pervading the international security environment reflect this master list, and it is difficult to deny it contains a number of things that will probably pose a problem for someone, somewhere, at some point in time. But such lists are little more than a grab-bag of beliefs and tactics (terrorism); capabilities (WMDs and ballistic missiles); interpretation of political conditions (failed states, or the current descriptor, "fragile" states); and broad trends (e.g., in demographics, the prevalence of infectious disease, and growing resource scarcity). In their generic approach, these lists fail to answer the question that ought to be the starting point for any threat assessment: who is threatening whom, and why?

By this definition, people threaten people; states threaten states. The means involved are nothing more than a way of carrying out the threat. Threats to national security are also target-dependent; they are conceived in the "eye of the beholder," in this case the individual nation-state, and depend upon a threat relationship with the originator of the threat – a "threatener," for lack of a better term, possessed of both the capability to carry out a threat, and the desire to do so. If security environment analysis is decoupled from the discipline imposed by the requirement to relate threats to the "national security state," however, it becomes more difficult for decision-makers to differentiate between threats, risks, trends and challenges. The resulting lack of clarity is best illustrated by the epistemic confusion evident in contemporary security analysis, where the threat posed by, for example, al Qaedism has proven resistant to definitive

12 *A More Secure World: Our Shared Responsibility* (Report of the Secretary General's High Level Panel on Threats, Challenges and Change), p. 23. (http://www.un.org/secureworld/) Accessed 4 July, 2007.

characterization, whereas the "threat" of climate change is increasingly accepted as dogma.

Consider, for instance, the July 2007 National Intelligence Estimate on the terrorist threat to the US homeland. Declassified key judgments state that the "US Homeland will face a persistent and evolving terrorist threat over the next three years. The main threat comes from Islamic terrorist groups and cells, especially Al Qaeda, driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities." Noting that counterterrorism measures "have helped disrupt known plots against the United States since 9/11," the NIE warns, "this level of international cooperation may wane as 9/11 becomes a more distant memory and perceptions of the threat diverge."[13]

Why should they diverge, especially among Western allies? Much has been made of the different perceptions that Americans and Europeans (and perhaps Canadians) have of the terrorist threat, and what to do about it. Many commentators cling to the belief that the United States has overreached by advocating and implementing a military response to 9/11; they argue that the Bush Doctrine has mistakenly drawn connections between disparate terrorist groups and rogue states such as Iran, Libya and Saddam's Iraq. Europeans, it is suggested, put more effort into trying to counter the "root causes" of terrorism, arguing that military responses only make matters worse. Whether these different perceptions are formed by America's "Hobbesian Chaos" view of the world as opposed to Europe's Kantian "Perpetual Peace" view is a subject of some debate, but it certainly affects how the terrorist threat is perceived in relation to other "threats."[14]

In fact, this divergence is a superficial characterization because, on closer examination, identifying "root causes" turns out to be an inherently subjective exercise. For example, the European Counter-Terrorism Strategy, adopted by the European Council in November 2005, calls for action against "root causes" of "radicalization and recruitment." The Strategy states, "There is a range of conditions in society which may

---

13 The NIE can be accessed at (http://www.whitehouse.gov/news/releases/2007/07/20070717-2.html) Accessed 1 September 2007.

14 Robert Kagan focussed on the different perceptions of the role of power in today's international system in *Of Paradise and Power: America and Europe in the New World Order* (New York: Alfred A. Knopf, 2003).

create an environment in which individuals can become more easily radicalised. These conditions include poor or autocratic governance; rapid but unmanaged modernisation; lack of political or economic prospects and of educational opportunities."[15] However, the EU is not alone, as the United States National Strategy for Combatting Terrorism also identifies four "root causes:"

i. Political alienation;

ii. Grievances That Can be Blamed on Others;

iii. Subcultures of Conspiracy and Misinformation and;

iv. An Ideology That Justifies Murder.

The US Strategy also articulates a response: "The long-term solution for winning the War on Terror is the advancement of freedom and human dignity through effective democracy."[16]

These long-term appreciations of the threat's "root causes" are necessary to drive high-level strategic direction and international cooperation with respect to counter-terrorism. Differences in focus mean that a coherent high-level international focus on the terror threat is proving difficult to sustain, even among Western allies that have suffered civilian casualties in terror attacks.[17] However, while there are differences between the European tendency to emphasize "conditions" and the American tendency to emphasize ideology at the strategic level, there is evidence

---

15 Council of the European Union, *The European Union Counter-Terrorism Strategy*, 30 November 2005. The Strategy states the following as "key priorities" in the prevention of recruitment and radicalization:
- Develop common approaches to spot and tackle problem behaviour, in particular the misuse of the internet;
- Address incitement and recruitment in particular in key environments, for example prisons, places of religious training or worship, notably by implementing legislation making these behaviours offences;
- Develop a media and communication strategy to explain better EU policies;
- Promote good governance, democracy, education and economic prosperity through Community and Member State assistance programmes;
- Develop inter-cultural dialogue within and outside the Union;
- Develop a non-emotive lexicon for discussing the issues;
- Continue research, share analysis and experiences in order to further our understanding of the issues and develop policy responses.

16 *United States National Strategy for Combatting Terrorism*, September 2006 (http://www.whitehouse.gov/nsc/nsct/2006/), pp. 9-10.

17 David Omand, "Countering International Terrorism: The Use of Strategy," *Survival*, Vol. 47, No. 4, Winter 2005-2006, pp. 107-116.

of considerable agreement among western allies that 9/11 demonstrated the existence of a new type of threat, at least in terms of scale and potential for destruction.[18] As a result, governments on both sides of the Atlantic continue to adjust their national security policies, legislation and practices in order to provide for earlier and more efficient cooperation between intelligence and law enforcement in terrorism cases. European and American views may differ, but their respective approaches to terrorism, while perhaps rhetorically divergent, have much in common.[19]

Some of that convergence began before 9/11, when Canada and its allies in the North Atlantic Treaty Organization began to reconsider what role collective defence measures have in the post-Cold War/pre-9/11 threat environment. NATO's 1999 Strategic Concept pointed to the growing threats of terrorism and the proliferation of weapons of mass destruction, and Article V of the Washington Treaty was invoked after 9/11, thereby declaring them "attacks against us all."[20] The significance of NATO's response lies in the acknowledgement that attacks of such scale and impact were not simply criminal acts: they were attacks on the West, and collective defence measures have been part of the response. 9/11, however, was the key trigger in the development of new Western security policies and strategies focussing on the new security environment. For the European Union, that meant adopting a counter-terrorism strategy that included the European Arrest Warrant, enhancement of police and judicial cooperation, measures to counter terrorist financing, a common definition of terrorism, and a Framework decision to punish terrorism offences with heavier sentences than common criminal offences. After the Madrid bombings in March 2004 (3/11), the European Union also created a position of Counter-Terrorism Coordinator to assist in intelligence sharing and coordination. While it must always be remembered that Europe-wide policies and strategies are subject to the interpretation and implementation of Member States, it was no mean feat for those states, traditionally wary of losing autonomy in Justice and Home Affairs, to recognize the need to act quickly in these areas after 9/11 and, subsequently, even more so after 3/11.[21]

---

18 For a view of how US and European approaches to terrorism and proliferation are tilting toward convergence more than divergence, see Anna I. Zakharchenko, "The E.U. and U.S. Strategies Against Terrorism and Proliferation of WMD:A Comparative Study (George C. Marshall European Center for Security Studies, Occasional Paper No. 6, January 2007)

19 A useful review of some of these developments is provided in Michael Jacobson, *The West at War: U.S. and European Counterterrorism Efforts, Post September 11* (Washington: The Washington Institute for Near East Policy, 2006)

20 "NATO and the Fight Against Terrorism," (http://www.nato.int/issues/terrorism/index.html) Accessed 2 December 2007.

21 Oldrich Bures, "EU Counterterrorism Policy: A Paper Tiger," *Terrorism and Political Violence*, (2006) Vol. 18, pp. 71-73.

Returning to the "context is everything" axiom, no discussion of the security environment is complete without recognizing that different opinions exist about what constitutes a "threat" to Western security, and more specifically to Canada's security. Nonetheless, all governments must sort out "threats" from "challenges" because of competition for "strategic" resources and focus. It may prove difficult to remain focused on the Al Qaedist threat in the face of impassioned calls to mobilize state resources to meet challenges that are couched in the language of threats. For instance, in April 2007, a blue-ribbon panel of retired American senior military officers released a report examining how climate change poses a "serious threat" to America's national security. The panel also found that "climate change, national security and energy dependence are a related set of global challenges." It concluded that the United States should act quickly to "help stabilize climate changes at levels that will avoid significant disruption to global stability and security."[22]

Is it appropriate to frame climate change using the language normally reserved for enemies plotting our demise? Is climate change really a threat? If so, to whom? Can the United States really "stabilize climate change?"

Yet, action is what the military panel proposes, based on the assertion that climate change is at once a national security "threat" and a component of interdependent global "challenges" that includes the connection between energy dependence and national security. Again, though, should we frame potential climate changes as a threat, in the same way that we think of terrorists or rogue states?

Clearly, framing climate change as a threat has serious implications, since doing so may lead to political pressure to act on the basis of inconclusive or exaggerated evidence. Significantly, in the United States, the intelligence authorization act for 2008 includes the requirement for the Director of National Intelligence to produce a National Intelligence Estimate on the "geopolitical and security implications of climate change."[23] The American intelligence community is now mandated to gaze into the future to consider the presumed effects (geopolitical and security implications) brought about by a presumed cause (climate change). Is this a good idea?

---

22 Walter Pincus, "Intelligence Chief Backs Intelligence Study," *Washington Post*, 12 May 2007 (http://www.washingtonpost.com/wp-dyn/content/article/2007/05/11/AR2007051102375.html) Accessed 5 June 2007.

23 *Ibid*

More importantly, is it a wise expenditure of national security resources? There are threats of a much more immediate, and far better understood, nature. These threats should not be confused with "dangers," "risks," or "challenges," in part because threats imply an enemy, and thus are of such consequence that governments are obliged to respond. After all, if climate change is framed as a "threat," how can action not be taken? For that matter, why was action not taken in response to warnings in the mid-1970s of an impending ice age? Might not it be easier and cheaper, as economist Bjorn Lomberg has suggested, to adapt to climate change, rather than attempt to reverse it?[24]

These are important questions that analysts should pursue and investigate as they would any *challenge*. However, there are plenty of real national security *threats* (posed by real enemies, with strategic objectives and proven, lethal capabilities) to worry about for the foreseeable future – without the needless distraction of trying to design and take action against unsubstantiated, amorphous and non-sentient "threats." It is essential to sort threats from challenges because, in a world of genuine and intentional threats to Western security, undifferentiated, all-encompassing lists of threats, challenges, risks and dangers are not useful. In fact, they make it more difficult to focus on core national security matters.

And, unlike climate change, there is no way to "adapt" to the threat posed by Al Qaedists.

Understanding the Strategic Threat

At a time when the international community seems to be coalescing (at least rhetorically) around the inchoate "threat" of climate change, why is it so difficult to generate widespread agreement that al-Qaeda and its fellow travelers constitute a serious threat – particularly as they have already acted, and demonstrated intent, capability and a willingness to continue?

---

24 Ray Suarez interview with Bjorn Lomborg, "Author Says Redirect Resources Against Climate Change," PBS Online Newshour, 25 April 2007 (http://www.pbs.org/newshour/bb/environment/jan-june07/adaptation_04-25.html) Accessed 5 November 2007.

One reason is that, despite a series of attacks on western interests since the early 1990s, there remain those who assert that Al Qaeda, and the ideology it represents, pose merely a criminal law challenge rather than strategic threat to national security. It should come as no surprise that such a difference of opinion exists; terrorism is an inherently politicized subject. Even though the western allies have been involved in what has been variously termed the War on Terror, the Campaign Against Terrorism, the Fight Against Terror and the Long War since the attacks on the United States on September 11th, 2001 they have yet to reach agreement on the scope, dimensions or even the objectives of their counter-terrorism activities.

This disagreement is often related to the lack of an internationally accepted definition of terrorism. Why does defining terrorism pose such a chore? Is there any doubt that a deliberate, pre-planned act of flying airplanes into skyscrapers, with the obvious intent of inflicting as much damage and causing as much death as possible, could be anything but terrorism? There is no need to replicate the many definitions that exist -- the authors of one study published almost twenty years ago managed to scrape up 109 – but it is useful to consider what are generally accepted as terrorism's main components.[25] Bruce Hoffman approaches the challenge of definition by examining what distinguishes terrorism from criminals and guerrillas or insurgents. In doing so, he settles on terrorism's characteristics as follows:

- ineluctably political in aims or motives;
- violent – or, equally important, threatens violence;
- designed to have far-reaching psychological repercussions beyond the immediate victim or target;
- conducted either by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia) or by individuals or a small collection of individuals directly influenced, motivated or inspired by the ideological

25 Alex P. Schmidt and Albert J. Jongman et al. *Political Terrorism* (SWIDOC, Amsterdam and Transaction Books, 1988), p. 5.

aims or example of some existent terrorist movement and/or its leaders; and

- perpetrated by a subnational group or nonstate entity.

Hoffman then attempts to define terrorism as "the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change."[26]

This is a satisfactory definition of terrorism as a doctrine or system of belief and principles. It indicates that the complete picture of the terrorist is much different than that of the criminal. Motive should be central to any intellectually honest definition of terrorism, and it forms part of the definition of terrorism provided in Canada's Anti-Terrorism Act of 2001.[27] Nonetheless, an Ontario Superior Court of Justice ruling in 2006 struck down the so-called "motive clause" in the Canadian legislation as being in breach of Section 2 of the *Canadian Charter of Rights and Freedoms*, which includes as fundamental freedoms those of conscience, religion, thought, belief, opinion, expression, peaceful assembly and association. [28] Lord Carlyle, in his 2007 independent review of British terrorism legislation, stated: "In relation to the components of terrorist activity, I agree with the view that the true and definable characteristics of terrorism are to be found in the combination of motive and means of perpetration." He went on to recommend a change to the motive part of the definition in the UK's Terrorism Act, so as to include philosophical, racial and ethnic motives to those already identified, namely political, religious and ideological. [29]

It is in the confluence of motive and potential for violence directed either against the public, property or an essential service that makes terrorism a national security threat rather than just a crime. Strategic "threats" to

---

26 Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2006), p. 40.

27 The so-called motive clause" is part of Canada's Criminal Code definition of terrorist activity, which includes a number of offences, but also "an act or omission, in or outside Canada,
(i) that is committed
(A) in whole or in part for a political, religious or ideological purpose, objective or cause, and
(B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada." See Criminal Code (R.S., 1985, c. C-46), Part II. 1 "Terrorism", Section 83.01(1)(b)(i)(A) (http://laws.justice.gc.ca/en/showdoc/cs/C-46/bo-ga:l_II_1//en#anchorbo-ga:l_II_1) accessed 24 June 2007).

28 R. v. Khawaja (24 October 2006), 04-G30282 (Ontario Sup. Ct. of Justice).

29 Carlile, Lord of Berriew. "The Definition of Terrorism." A Report by Lord Carlile of Berriew Q. C. Independent Reviewer of Terrorism Legislation, Presented to Parliament by the Secretary of State for the Home Department, by Command of Her Majesty. March 2007, pp. 33-37.

national security require different responses than would be the case vis-à-vis "crimes" or "offences." However, there is little likelihood of reaching consensus on the current and future threat of transnational terrorism if allies fail to grasp the nature of, and relationship between, terrorism's criminal and strategic elements. The threat consists of both.

It is perhaps easier to think about terrorism as just another form of criminal deviancy; after all, we are dealing with actors at the sub-state level, and the actions they take in pursuit of their objectives necessarily **are** criminal. Terrorists may (and do) detonate explosives, attack railways, hijack airplanes and turn them into projectiles. These certainly are all criminal acts that may be prosecuted under the domestic criminal legislation of the states in which the acts take place. Ordinary criminals, however, who seek to profit from illegal acts, make mischief or cause havoc, have no discernible strategic objectives against the states within which they operate; this differentiates them from terrorists. Criminals may be motivated by goals other than greed or revenge, but while their behaviour contradicts our laws and values, it does not constitute a deliberate, organized challenge to the state per se, or to the legitimacy and standing of its government and laws. Crime and terror may ultimately share methods, but in terms of how individual acts affect the state, they differ greatly in their motivation, genesis and ultimate aims.

Although crime is most often an end in itself; terrorism is a means to an end, a method of effecting political change. In this sense, there are many types of "terrorisms."[30] Terror and threats of terror are often a means of seizing the initiative and extorting concessions to demands, and as such, they are used preferentially by those who pursue limited goals - e.g., "single-issue" terrorists. The threat posed by such terrorists is akin to that posed by organized criminals, and there are cases where organized criminals and terrorists may converge in many important ways. They share many operational characteristics, and may even work together for mutual benefit, and as a result, terrorist groups and organized crime syndicates can in some respects become indistinguishable. One study shows how this process has formed 'hybrid' terrorist/organized crime groups in Chechnya, the Black Sea region and the Tri-Border area of Peru, Paraguay and Argentina.[31] In these instances, individuals involved in enabling

30 Laqueur, Walter. "Postmodern Terrorism- New Role for and Old Game." *Foreign Affairs* Vol. 75, No. 5, p.25

31 Shelley, Louise I. and Picarelli, John T. "Methods and Motives: Exploring Links Between Transnational Organized Crime and International Terrorism." *Trends in Organized Crime*, Vol. 9, No. 2, winter 2005. pp. 52-68.

activities, such as fraud and extortion, take advantage of economic, social and political tumult to serve both terrorists and crime syndicates.

Conventional intelligence, legislation and law enforcement can generally manage these threats as routine business. It might even be appropriate, even preferable, to refer to such perpetrators as "modern-day pirates" instead of "terrorists" (let alone "militants" or "combatants").

However, successful action against the single-issue terrorist does not diminish the threat posed by transnational or strategic terrorism (the hallmark of jihadist organizations like Al Qaeda), because this brand of terrorism poses an aggregate threat to all western states and their common and individual interests. Al Qaeda's ideology of jihad seeks to use catastrophic violence – and the fear of it – to undermine, and ultimately supplant, the status quo. Whereas an act of violent crime or single-issue terrorism might result in devastating consequences either in terms of victims or damage to property, the scope and scale of the threat is usually limited. For "traditional" terrorist groups, such as the IRA, the ETA or the PKK, terror tactics and operations are conducted for limited, irredentist objectives (even though funding and logistical support might come from abroad). The Al Qaedists' objectives, by contrast, are not so limited.

Single-issue terrorists do not seek global strategic effects in the same way as might a bin Laden or a Zawahiri. Why? Unlike more modest "common" criminals and single-issue terrorists, al Qaedists are strategic terrorists with large-scale objectives pursued as a generational goal. They conduct operations with a view of forcing the West in general, and the United States in particular, to abandon the Middle East. In his September 2002 "Letter to America," Osama bin Laden even stated that Al Qaeda ultimately sought the Islamization of the United States which, in Martin Rudner's words, "would bring all other countries, Western as well as Muslim, under the sacralized rule of a globalized, triumphant, militant Islam."[32] The first stage of Zawahiri's global strategy seeks to restore the historic caliphates of Dar Al-Islam, replacing the "apostate" regimes of Saudi Arabia and Egypt with regimes that function according to an idiosyncratic and highly conservative interpretation (which is to say, their interpretation) of Islam. The second stage involves using the Caliphate as a base to "lead the Islamic world in a jihad against the West." There are

---

32 Rudner, Martin. "Challenge and Response: Canada's Intelligence Community and The War on Terrorism." *Canadian Foreign Policy*, Vol. 11, No, 2 (Winter 2004). pp.17-39.

several theatres in this global insurgency, including the Middle East, East Africa, the Americas and Western Europe.[33]

Alexander Downer, the former Australian Minister for Foreign Affairs, released a report in 2004 explaining to the public the nature and implications of the Al Qaedist threat, describing it succinctly:

> This form of transnational terrorism presents Australia with a challenge previously unknown. Its aims are global and uncompromising: to fight its enemies wherever it is able, and ultimately to establish a pan-Muslim super-state. Its battlefield is also global. And it strives, where it can, for large scale, maximum casualty impact. We saw this on 11 September 2001. We felt it a year later in Bali.[34]

There is little uncertainty about Al Qaeda's goals and methods; innumerable texts have been written describing both. For example, Zawahiri's "Jihad, Martyrdom, and the Killing of Innocents," justifies the use of terrorist tactics such as suicide bombings in pursuit of war aims.[35] In 2007, Zawahiri called for the "holy war" in Iraq to be extended throughout the Middle East toward the creation of a "greater Syria."[36] Western governments may differ on how to frame the "war," "campaign" or "struggle" against terror and/or terrorists; bin Laden and his ideological fellow-travelers seem much more coherent about what they hope to achieve, and why.

There are, however, some commentators who insist that Al Qaedists have no coherent strategy whatsoever. In this school of thought, 9/11 was not a rational Clausewitzian political act based on calculated assessments of cause and effect but rather the playing out of a fantasy ideology to be guided by the "will of God." This argument is based largely on the assumption that it is entirely unrealistic for a diminutive group such as Al Qaeda to expect to "defeat" a country like the United States.[37]

---

33 David J. Kilcullen, Countering Global Insurgency," *The Journal of Strategic Studies*, Vol.28, No. 4 (August 2005), pp. 598-599.

34 Government of Australia, *Transnational Terrorism: The Threat to Australia* (Canberra: Commonwealth of Australia, 2004) p. vii

35 Raymond Abrahim (Editor and Translator), *The Al Qaeda Reader* (New York: Doubleday, 2007), pp. 141-171.

36 Uzi Mahnaimi, "Al-Qaeda Chief Urges Iraqis to Export Jihad," *Times Online* (www.timesonline.co.uk), 27 May, 2007.

37 Harris, Lee. "Al Qaeda's Fantasy Ideology." *Policy Review*, Hoover Institution, Stanford University. August & September 2002, 14 pages.

But is the expectation so unrealistic? Given that Al Qaedists could point triumphantly to the expulsion of the Soviet Red Army from Muslim lands in Afghanistan, why would they think it inconceivable that the United States and the West in general could not be worn down over time, and forced to leave the Middle East? Osama bin Laden apparently believed that the small and ineffective "Arab Afghan" presence in Afghanistan, not the relentless US-backed mujahideen, actually turned the tide against the Soviets.[38] Even if this "fantasy ideology" characterization of Al Qaeda is accepted, however, that makes the threat posed by Al Qaedists no less dangerous.

While it may be inappropriate to speak of Al Qaedists as "warriors," they nonetheless often operate in a fashion consistent with military operational practices and discipline, and – at the strategic level, at least – they usually have more than piracy or crime-for-profit in mind. Their terrorist tactics are an integral part of a campaign aimed at attaining political and strategic objectives. They also inspire isolated, like-minded individuals and so-called "autonomous terror cells" to sympathetic acts of terror. While not necessarily organized and directed by a centralized command and control system, these groups and individuals are roused and motivated by Al Qaeda's example to attack targets throughout the West. The individuals allegedly planning attacks on soldiers in Fort Dix, New Jersey and on John F. Kennedy International Airport in 2007 would fall into this category.[39] Commentators, who insist that the terrorist threat is "hyped," and dismiss the risk of being killed by terrorists as statistically insignificant, appear not to understand the nature of a strategic threat: the "attack" is only part of the terrorist repertoire.[40]

Consider, for instance, the Al Qaeda-inspired terrorists who carried out the Madrid train bombings in March 2004, and who succeeded in changing the outcome of the subsequent federal election, and the course of Spanish foreign policy. Al Qaeda's offer of a truce thereafter to other European nations if they followed suit shows a degree of strategic

---

38 Lawrence Wright, *The Looming Tower: Al-Qaeda and the Road to 9/11* (New York: Alfred A. Knopf, 2006), p. 145.

39 Dale Russakoff and Dan Eggen, "Six Charged in Plot to Attack Fort Dix: 'Jihadists' Said to Have no Ties to Al Qaeda," The Washington Post, May 9, 2007, p. A1 (http://www.washingtonpost.com/wp-dyn/content/article/2007/05/08/AR2007050800465.html) Accessed 8 August 2007.
Anthony Faiola and Steven Mufson, "N.Y. Airport Target of Plot: Officials Say 3 Held in Alleged Plot to Bomb JFK," The Washington Post, June 3, 2007, p. A1 (http://www.washingtonpost.com/wp-dyn/content/article/2007/06/02/AR2007060200606.html) Accessed 6 August 2007.

40 John Mueller, "Is There a Terrorist Threat: The Myth of the Omnipresent Enemy," *Foreign Affairs* (September/October 2006)

acumen,[41] as does dividing the United States and its coalition allies in Afghanistan and Iraq might have little military impact, but it certainly eats into the perception of American legitimacy: Anti-Americanism and resentment of US power can potentially drive politics in many countries.

Even if such "remotely-inspired" terrorists are unsuccessful (either due to effective intelligence and law enforcement, or their own lack of capacity), there is no denying that they pose a violent immediate threat and that they also support the Al Qaedist ideology. Successful attacks in this vein, in addition to achieving the terrorists' immediate objective of sowing mayhem, can trigger economic chaos or induce governments to alter policies. They also have the objective to incite other like-minded individuals to violence, and further embolden sponsoring states that, like Iran, share their hatred of the US and the West. Clearly, these individuals and organizations possess both the capability and the intention to cause harm, and have a well-documented record of doing so – the key characteristics of a "threat."

Framing the contemporary terrorist threat requires that we understand that while it displays many of the characteristics of criminal activity, its perpetrators seek grander goals – up to and including a fundamental restructure of the international status quo. As the United States is the main guarantor of international stability, it was logical for Osama bin Laden to select America for his February 1998 declaration of war, declaring it a religious obligation to attack Americans and their allies whenever and wherever possible (including through the use of weapons of mass destruction). His threat, and that posed by Al Qaedists writ large, has proven to be a truly strategic menace to the security of the West, and therefore worthy of a strategic response.

It is imperative that the strategic nature of the contemporary terrorist threat be understood. The ideology of jihad is every bit as opposed to Western liberal democracy as communism was during the Cold War. In the western democracies, more citizens may indeed die in accidental falls than terrorist attacks, but such statistical equivocation misses the point: extremist enemies do not have to be numerous to cause peril, and every success emboldens their fellows, while garnering additional support for their cause. That is why it is no longer the case that only states can threaten other states with strategic intent.

---

41 Mark Burgess, "Explaining Religious Terrorism Part 2: Politics, Religion and the Suspension of the Ethical" (Center for Defence Information, 23 August 2004) (http://www.cdi.org/friendlyversion/printversion.cfm?documentID=2384)

The use of the adjective "strategic" in this way denotes the nature of the threat posed by Al Qaedists. If we accept that their objective, or "policy," is to establish regimes that either actively support, or at least do not oppose, their interpretation of Islam, with a view to eventually re-establishing the "Caliphate", it follows that their "strategy" is the plan through which they seek to implement that goal. Their "strategy" might include trying to coerce governments into changing their foreign policies vis-a-vis Muslim countries in order to facilitate realization of the ends they seek.[42] Attacks, or the threat thereof, are thus not ends in themselves but rather a means to an end. What appears to be their madness is, in point of fact, their method.

While counter-terrorism operations certainly have dealt a blow to Al Qaeda, the group and the ideology it has inspired is not receding. In fact, as terrorism expert Paul Wilkinson has argued, it will remain a threat for decades to come. "Even if the current leadership is removed from the scene, there are likely to be eager successors in the wings ready to pursue the same overall objectives and using terrorism as a weapon. Whoever assumes the leadership, it seems almost certain that they will retain the key elements of Al Qaeda's ideology and combat doctrine, and hence will continue to wage their jihad within the front-line countries (Iraq, Afghanistan, Pakistan, Saudi Arabia), and by urging their networks within western countries to launch terrorist attacks on the homelands of the Coalition allies, including, of course, the US and UK."

And, of course, Canada. It is beyond doubt that Canada is another Coalition ally being eyed by Al Qaeda. In a November 2002 message broadcast on al-Jazeera, Osama bin Laden mentioned Canada in a list of countries targeted for being involved in Operation Enduring Freedom. The threat of retaliation for supporting US foreign policy is a propaganda tool available to Al Qaeda: Australia was also mentioned in the above broadcast, with bin Laden stating that Australia "ignored the warning until it woke up to the sounds of explosions in Bali."[43] Canada's involvement in Afghanistan was of course only a pretext for him to issue such warnings as, even before 9/11, Sunni Islamic militant groups were threatening Canada.[44]

---

42 Jessee, Devin D. "Tactical Means, Strategic Ends: Al Qaeda's Use of Denial and Deception." *Terrorism and Political Violence*, 2006, Vol. 18, pp. 367-388.

43 BBC Monitoring, "Full Text: 'Bin Laden's Message,'" (http://news.bbc.co.uk/2/hi/middle_east/2455845.stm) Accessed 4 August 2007.

44 Rudner, Martin. "Challenge and Response: Canada's Intelligence Community and The War on Terrorism" *Canadian Foreign Policy*, ISSN 1192-6422, Vol. 11, No, 2 (winter 2004). pp.17-39.

The threat is not receding. In November 2007, the Chairman of Lloyd's of London, Lord Peter Levene, stated that "Canada's risk profile has changed in recent years and while no stranger to terrorism, intelligence suggests that its role is shifting from a hub for fundraising and planning attacks outside the nation – for example in the U.S. – to a credible target in its own right...."[45] There is other evidence that the threat to Canada is more pronounced.[46] Bin Laden's clever use of intimidation to have us change our foreign policy – including support for the NATO alliance in Afghanistan – demonstrates the practical implications of what Rohan Gunaratna identifies as Al Qaeda's strategic, as opposed to apocalyptic, perspective: "Contrary to popular belief... Al Qaeda has never sought an apocalyptic goal. Closer examination suggests that it is a very practical group, with clear aims and objectives, but one that is capable of chameleon-like manoeuvring."[47] Indeed, it is easy to see the Al Qaeda's list of grievances as endlessly mutable: bin Laden's ire over the presence of US troops in Saudi Arabia has now morphed into a peculiar obsession with a rather diverse array of provocations, ranging from the Crusades and the Reconquista, to globalization, class and capitalism.[48]

Conclusion

Back to the "context is everything" axiom, it is not enough simply to differentiate between terrorism and crime as abstract entities; we must also differentiate between traditional "terrorism" and the international terrorism we now face. As Walter Lacquer points out, even 9/11 was only a step toward what could come to pass, "megaterrorism" characterized by the use of weapons of mass destruction.[49]

It is crucial that we understand how terrorism fits into today's national security context, not that of 1985. Part of that context involves considering how Canada, as a country, sizes up the terrorist threat as a matter of strategic import alongside others worthy of national attention. As climate change seems easily cast in Manichaean terms akin to the Cold War struggle of good against evil (i.e., environmental activists versus those

---

45 Tara Perkins, "Canada Coming into Terrorists' Crosshairs: Lloyd's," *Globe and Mail*, 28 November 2007 (http://www.globeinvestor.com/servlet/story/RTGAM.20071128.wlloyds1128/GIStory/) Accessed 29 November 2007.

46 See, for instance, this year's global risk findings of Janusian Security Risk Management (http://www.riskadvisory.net/news/62/81/) Accessed 10 December 2007.

47 Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror*, (New York: Columbia University Press, 2002), p. 94.

48 Fawaz A. Gerges, "Bin Laden's New Image: Younger, More Marxist," *The Christian Science Monitor*, 13 September 2007 (http://www.csmonitor.com/2007/0913/p09s01 coop.htm) Accessed 14 September 2007.

49 Walter Lacquer, "The Terrorism to Come," *Policy Review*, August and September 2004.

"contributing" to climate change), the public focus on this struggle seems to have affected the perception of many Canadians. This is reflected in a December 2007 poll, in which thirty six percent of respondents identified climate change as the world's biggest threat, while only eleven percent said so of terrorism.[50] Based on this evidence, Canadians seem not to be deeply concerned about terrorism. In a poll conducted just four months earlier, however, fully 64 percent of Canadians claimed to believe that terrorists could try to gain access to weapons of mass destruction from Russia, with almost as many fearing that Russian weapons scientists could conceivably work their trade for terrorists groups.[51] The contrast between these two polls may be explained as simply different cognitive approaches taken to grapple with abstract, as opposed to potential "real world" threats.

But it is also critical not to conflate all "real world" terrorist threats – historical and contemporary -- as equivalent in terms of how we should frame and respond to them. Historical analogies can have indisputable heuristic value for analysts and decision-makers alike, but, again, we must revert to the centrality of context. While Sikh terrorism was never a direct strategic threat to Canada, today's Al Qaedist threat is a very different beast.

It is nonetheless worthwhile to discuss and understand why it is just as difficult today (as in 1985) to advance wider public appreciation of just how significant the threat is, and why dealing with it simply from a criminal justice point of view is not sufficient. The Inquiry's Terms of Reference are geared toward achieving a better understanding of why the massive Air India criminal trial, which unfolded over many months and at great cost, ended without convictions. That part of the Inquiry's work by necessity invites a focus on the underlying factors that govern the preparation and presentation of criminal cases dealing with terrorist incidents or allegations. However, counterterrorism strategy must take into account more than just how to mount and execute successful criminal prosecutions: it must also provide for the ability of the state to deter or prevent further hostile acts. That is why we must understand the strategic nature of the Al Qaedist threat, and how it differs from events like the Air India bombing.

---

50 Marcus Gee, "Poll Highlights Unease Over US Foreign Policy," *Globe and Mail*, 11 December 2007 (http://www.theglobeandmail.com/servlet/story/LAC.20071211.POLL11/TPStory/Business/columnists) Accessed 11 December 2007.

51 Jack Aubry, "Canadians Fear Terrorist Access to Russian WMDs: Poll,", 23 August 2007 (www.canada.com) accessed 23 August 2007.

In retrospect, it is likely that the Air India bombing incidents fit better on the "criminal" end of a spectrum of threats to Canada; the Al Qaedist threat that we face today, and that will persist into the future, is much closer to the "war" end of the spectrum. Should the same rules apply to both ends of this spectrum?

How today's threat is framed (i.e., either primarily as a strategic war-like threat or a criminal challenge) will determine what must be emphasized when making recommendations in regard to the Inquiry's mandate, especially on the evidence/intelligence relationship. If it is accepted that Al Qaedists present a strategic, and not just purely criminal, threat to Canada and its allies, then it is suggested that a simple question should be asked before making any recommendations affecting Canada's national security system: In terrorist investigations, which of the following is more important: Securing convictions? Ensuring a fair trial? Or preventing further attacks? From a strategic point of view, the last consideration deserves most weight, because the terrorists we face are best understood as an adversary, over whom we must maintain tactical advantage. Winning the fight will require the use of many of the state's instruments of power (i.e. military, political, economic, diplomatic, legal and financial), but we must guard against weaknesses in the system that terrorists can exploit. The necessity of maintaining tactical advantage over our adversaries should be kept in mind, especially when considering recommendations related to RCMP-CSIS relations and the critical issue of the relationship between evidence and intelligence. Recalling that national security is best understood as a complex system, we must guard against making changes to one part of the system that would compromise the effectiveness of another.

After all, as Judge Richard Posner observes:

> As with so many legal dichotomies, that of "crime" versus "war" does not fit an emergent reality, in this case that of global terrorism. It is an occupational hazard of lawyers to stall in their consideration of issues at the semantic level. Rather than ask whether modern terrorism is more like crime or more like war and therefore which box it should be put in, one should ask why there are different legal regimes for crime and war and let the answer guide the design of a sensible

> regime for fighting terrorism. It is not war as such but the dangers created by war that explain and justify a curtailment of civil liberties in the waging of war. A similar curtailment may be justified by the dangers posed by terrorists avid to acquire weapons of mass destruction.[52]

Our ability either to deter an attack today, or to respond properly in the event of one occurring, will have an impact on a global insurgency rather that on a single nationalist/separatist campaign. As former British intelligence official David Omand has commented regarding the tensions inherent to the co-existence between secret intelligence and an adversarial court system in that country, "a global intelligence capability... would be severely hampered if all operational counter-terrorist intelligence had to be managed, recorded and transcribed according to our strict rules of evidence just in case it might one day be relevant to a prosecution."[53] This common sense reminder is worthy of our attention, especially as the stakes continue to grow in an age wherein individuals and small groups have the potential capability and motivation to cause so much destruction.

In other words, context is everything, and we must be aware of the insufficiency of making a direct comparison between what may or may not have worked to deter, investigate or prosecute the perpetrators of the 1985 attacks and what may be required today. As a result, while it may be tempting to describe the bombing of Air India Flight 182 as "Canada's 9/11," such a characterization is not warranted. It is a more judicious reading of history to state that Air India was Canada's Air India; 9/11 - as is the case for all Western nations who find themselves in Al Qaeda's sights – was also Canada's 9/11.

---

52 Richard A. Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (New York: Oxford University Press, 2006), pp. 72-73.

53 David Omand, "Security Dilemmas," *Prospect Magazine*, Issue 129, December 2006. For a view of the international dimensions of international cooperation, see Stephane Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," in *International Journal of Intelligence and CounterIntelligence*, vol. 16, 2003, pp 527-542.

Appendix A

Extract from the Terms of Reference for the Commission of Inquiry into the Bombing of Air India Flight 182

i. if there were deficiencies in the assessment by Canadian government officials of the potential threat posed by Sikh terrorism before or after 1985, or in their response to that threat, whether any changes in practice or legislation are required to prevent the recurrence of similar deficiencies in the assessment of terrorist threats in the future,

ii. if there were problems in the effective cooperation between government departments and agencies, including the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, in the investigation of the bombing of Air India Flight 182, either before or after June 23, 1985, whether any changes in practice or legislation are required to prevent the recurrence of similar problems of cooperation in the investigation of terrorism offences in the future,

iii. the manner in which the Canadian government should address the challenge, as revealed by the investigation and prosecutions in the Air India matter, of establishing a reliable and workable relationship between security intelligence and evidence that can be used in a criminal trial,

iv. whether Canada's existing legal framework provides adequate constraints on terrorist financing in, from or through Canada, including constraints on the use or misuse of funds from charitable organizations,

v. whether existing practices or legislation provide adequate protection for witnesses against intimidation in the course of the investigation or prosecution of terrorism cases,

vi. whether the unique challenges presented by the prosecution of terrorism cases, as revealed by the prosecutions in the Air India matter, are adequately addressed by existing practices or legislation and, if not, the changes in practice or legislation that are required to address these challenges, including whether there is merit in having terrorism cases heard by a panel of three judges, and

vii. whether further changes in practice or legislation are required to address the specific aviation security breaches associated with the Air India Flight 182 bombing, particularly those relating to the screening of passengers and their baggage.

Peter Archambault holds a BA and MA from the University of New Brunswick, and received his PhD in History from the University of Calgary in 1997. Between 1998 and 2002, he was Director of Research for the Minister's Monitoring Committee on Change in the Department of National Defence and the Canadian Forces (MMC). The MMC provided oversight and reported to the Minister and public on reforms to DND and the CF that arose from several inquiries in the 1990s into matters such as military justice, military education and operations. In addition to supporting the Chair and Committee members in the research, analysis and drafting of five public reports, he assisted the Chairman, the Honourable John A. Fraser, in his role as Special Advisor to the Minister on Land Force Reserve Restructure. In 2000, that advice was presented in the report *In Service of the Nation: Canada's Citizen Soldiers in the 21st Century*.

In July 2002, Dr. Archambault joined the Center for Operational Research and Analysis in the Department of National Defence as a Strategic Analyst. He has since served in the Directorate of Strategic Analysis (D Strat A) in the Policy Group at National Defence Headquarters in Ottawa. He served as the NATO/European Union analyst, and was the co-editor of *Strategic Assessment* 2004 and 2005, a Departmental document that analyzes global security trends.

In September 2005, he joined the Strategic Analysis team supporting force development in the Strategic Planning Division. His work included providing analysis of the security environment and forecasting trends; developing domestic and continental scenarios; and exploring new and emerging defence and security concepts.

He is currently serving as a Strategic Analyst in Canada Command Headquarters.

In addition, he is an Adjunct Associate Professor of War Studies at the Royal Military College of Canada. Over the past ten years, he has taught courses in military history, intelligence analysis and Canadian security and defence policy.

In 2002, Dr. Archambault was awarded the Golden Jubilee Medal for his contribution to Canada.

BUILDING CANADA'S COUNTER-TERRORISM CAPACITY: A PROACTIVE ALL-OF-GOVERNMENT APPROACH TO INTELLIGENCE-LED COUNTER-TERRORISM

Martin Rudner
Distinguished Research Professor Emeritus
The Norman Paterson School of International Affairs
Carleton University, Ottawa

PURPOSE

The purpose of this study is to formulate the architecture for an all-of-government approach to countering terrorist threats, designed to support coordinated, intelligence-led interventions into the cycle of terrorist activities.

BACKGROUND

The terrorist attacks of 11 September 2001 catapulted counter-terrorism to the forefront of Canada's Security and Intelligence priorities. To be sure, Canada had experienced terrorist attacks previously in its history, most notably the bombing of Air India flight 182. Nevertheless, it was in the aftermath of September 11th that the Government of Canada moved swiftly to introduce a National Security Policy, enact Anti-Terrorism legislation conferring new and far reaching powers on the Security and Intelligence (S&I) services, and allocate substantially additional budgets to the departments and agencies concerned in order to build capacity to sustain their counter-terrorism efforts.[1] Yet, it is pertinent to note that these policy, legislative and budgetary initiatives were not accompanied by any review of the architecture of the Canadian S&I Community to assess its structural appropriateness for the contemporary counter-terrorism mission. Certain bureaucratic reorganizations were indeed undertaken, in particular the 2003 merger of disparate units into a singular Department of Public Safety and a Canada Border Services Agency; the formation of the Integrated Threat Assessment Center (ITAC) in October, 2004; and the creation of Royal Canadian Mounted Police (RCMP) Integrated National Security Enforcement Teams (INSET) involving partnering with other intelligence and law enforcement services at the local, tactical level. However the core architecture and particular roles and operational principles of the various components of Canada's S&I community remained -- and remains – by and large intact and untouched by the evolving threat environment.

---

1 On Canada's post-September 11th respond to the international terrorist threat environment, see Martin Rudner, "Challenge and Response: Canada's Intelligence Community and the War on Terrorism," *Canadian Foreign Policy*, Vol. 11, No. 2 (2004); David Daubney, Wade Deisman, Daniel Jutras, Errol Mendes, Patrick Molinari, eds., *Terrorism, Law & Democracy: How is Canada Changing Following September 11* (Montreal: Les Editions Thémis, Faculté de droit, Université de Montréal, 2002).

By way of contrast, Canada's principle allies in international intelligence relations, the United States, United Kingdom, and Australia all undertook far-reaching reviews of their intelligence systems during the first half of this decade, prompted by intelligence failures associated with the September 11th attacks and the subsequent Iraq Weapons of Mass Destruction debacle. These reviews were conducted independently of their respective intelligence communities, by a congressional committee and independent national commissions in the United States[2], and by official commissions of inquiry in Australia[3] and the United Kingdom[4]. All these reviews came forth with proposals for reforming their respective national security architecture and intelligence functions. In December of 2007, the U.K Home Office, the ministry responsible for national security, commissioned a report by DEMOS, a preeminent think-tank, exploring the transformations required to equip government and the Intelligence community to meet the challenges of the contemporary threat environment. The report stipulated a need to adopt "a holistic approach to national security based on systems-thinking" to encourage "individuals, agencies, and departments to take a much broader perspective than normal".[5] This recommended all-of-government approach to national security would presage a more comprehensive and systematic perspective on the threat environment:

> 'This includes seeing overall structures, patterns in cycles and systems rather than identifying only specific events or policy options."

An analysis of the aforementioned reports and their recommendations underscores their preoccupation with promoting a paradigm shift in the

---

2 National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (New York: W.W. Norton & Co., n.d.)[2004]; Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington, DC: US Government Printing Office, 2005). See also Richard Posner, *Uncertain Shield: The U.S. Intelligence System in the Throes of* Reform (Lanham, MD: Rowman & Kittlefield, 2006); Jennifer Sims "Understanding Friends and Enemies: The Context for American Intelligence Reform," in Jennifer Sims & Burton L. Gerber, eds., *Transforming U.S. Intelligence* (Washington, D.C: Georgetown University Press, 2005), Arthur Hulnick, "U.S. Intelligence Reform: Problems and Prospects" *International Journal of Intelligence and CounterIntelligence*, Vol. 19, No. 2 (2006) and "Intelligence Reform 2007: Fix or Fizzle? *International Journal of Intelligence and CounterIntelligence*, Vol. 20, No. 4 (2007).

3 Sir Philip Flood, *Report of the Inquiry into Australia's Intelligence* Services (Canberra: Government of Australia, 2004).

4 The Rt. Hon. The Lord Butler of Brockwell, Report of a Committee of Privy Counsellors, *Review of Intelligence on Weapons of Mass Destruction*, HC 898 (London: The Stationery Office 14th July 2004).

5 Charlie Edwards, *National Security for the Twenty-first Century* (London: DEMOS, 2007)

traditional architecture of national security affecting, in particular, (a) the coordination of national intelligence efforts; (b) the strengthening of analytical capabilities; (c) improving intelligence sharing among the national security system; and (d) connecting intelligence to law enforcement. Each of these proposed reforms represents a rebalancing between traditional intelligence precepts, developed since the First and Second World Wars and refined during the Cold War, and the perceived imperatives for dealing with the contemporary threat environment. Thus, the issue of "coordination" touches on the balance between centralization and decentralization of control over the activities of intelligence services. Traditionally, intelligence services in democracies retain a high degree of decentralized control over their activities, subject, of course, to ministerial direction and oversight and statutory review. Any move towards strengthening coordination over the S&I community as a whole necessarily implies a greater centralization of direction over intelligence efforts, overriding the propensities of individual agencies. Creating a more robust "analytical capability" likewise denotes a building up of centralized functions, and a diminution of analytical roles in the subordinate agencies and departments. Improved "intelligence sharing" would tend to accentuate a holistic, centralizing approach to national security while blurring the uniqueness of individual agencies and even risking compromising their respective methods and sources. Linking intelligence to law enforcement could risk subordinating the operational secrecy of intelligence collection to the disclosure requirements of prosecution in courts of law.

The policy dilemma for designing an effective national security architecture is precisely to adapt intelligence precepts and the evolving operational requirements of counter-terrorism. Just as the effectiveness of intelligence operations may seem to depend on decentralized agency control, distributed analytical capabilities, distinctly cultivated sources and methods, and lawfully secret investigations, so effective counter-terrorism may call for more centralized coordination, integrated analytical capacity, enhanced intelligence sharing, and a robust connection between intelligence collection and law enforcement.

International terrorism remains a potent, deadly threat to Western democracies.[6] Almost every major democratic jurisdiction -- Australia, Belgium, Canada, Denmark, France, Germany, Great Britain, India, Indonesia, Italy, Israel, Netherlands, the Philippines, Spain, Sri Lanka, Turkey, the United States -- has been targeted with actual or foiled attacks.[7] The present Study explores ways to build up Canada's national security capacity to counter terrorist threats. The approach taken develops a paradigm for a re-designed national security architecture that responds to a functional analysis of contemporary international terrorism while also taking account of the mandated roles of Canada's S&I Community as a whole in addressing these threats. The commanding imperative is for Canada to act resolutely, proactively, effectively and lawfully to defeat terrorist threats to our national security and public safety, and also to friendly and allied countries.

The Study that follows will therefore focus through the analytical lens of a terrorism cycle, setting out the sequence of terrorist activities that precede and culminate in terror attacks on civilian targets. It then examines the scope for security and intelligence interventions at each stage of the terrorism cycle. Based on this analytical framework, the Study will proceed to consider the role of intelligence analysis in supporting a robust, calibrated, all-of-government approach to proactive, preventive interventions in the terrorism cycle. At the core of this all-of-government approach is the need for a coordination mechanism designed to ensure the coherent direction of the national counter-terrorism effort, consistent with the mandates and roles of the operational agencies representing the various intelligence and security disciplines.

---

6 Cf. J. Michael McConnell, Director of National Intelligence, *Annual Threat Assessment by the Director of National Intelligence for the Senate Select Committee on Intelligence*, 5 February 2008 (Washington, 2008). The most recent Canadian public assessment of terrorist threats is provided by the Canadian Security Intelligence Service, *Public Report 2004-2005* (Ottawa: Public Works and Government Services Canada, 2006), esp. pp. 1-7. See also Lorenzo Vidino, "The Tripartite Threat of Radical Islam to Europe," *inFocus*, Vol. 1, No. 3 (2007.

7 For recent surveys of international terrorist threats to countries in Asia, Europe, the Middle East and North America, see, *e.g.*, U.S. Department of State, Office of the Coordinator for Counterterorism, *Country Reports on Terrorism 2006* (Washington, DC: 2007), esp. chaps. 1 & 2; The Netherlands General Intelligence and Security Service, *Violent Jihad in the Netherlands Current Trends in the Islamist Terrorist Threat* (The Hague, 2006); Rohan Gunaratna, "Islamic Terrorism: Can We Meet the Challenge? *Global Asia*, Vol. 2, No. 3 (2007); Lorenzo Vidino, *Al Qaeda in Europe. The New Battleground for International Jihad* (Amherst, NY: Prometheus Books, 2006); Angela Rabasa *el al*, *Beyond al-Qaeda. Part 1 – The Global Jihadist Movement; Part 2 – The Outer Rings of the Terrorist Universe* (Santa Monica, CA: RAND, 2006).

References in this Study to religious- or ethnic-based terrorism should not be taken as suggesting that all individuals, organizations, and institutions of those communities are implicated in terrorism. Terrorists comprise a cadre of dedicated, extremist, militant individuals prone to violence. It is to these terrorist elements, and to their actions, that this Study refers.

3. THE TERRORISM CYCLE

International terrorism is predicated on a complex cycle of activities. The key enabling activities for international terrorist operations can be set out as follows:

- Strategic planning
- Recruitment of activists and operatives
- Training
- Communications
- Resourcing, financing, fund-raising and money transfers
- Procurement, preparation and delivery of materiel (including passports)
- Creating an infrastructure of safe houses, sleeper cells
- Propaganda and incitement
- Terrorist Penetration into Sensitive Government
- Department, Agencies and Institutions
- Tactical preparations
- Reconnaissance on targets
- Terrorist assaults on targets

Information about these activities is publicly available from an Al-Qaeda manual on terrorism, the *Encyclopaedia of the Afghan Jihad*,[8] which was introduced in evidence at the British trial in January, 2006, that convicted the radical Jihadist cleric Sheikh Hamza al-Masri of terrorism charges, and from other court cases and authoritative sources. In the decentralized organizational structure into which al-Qaeda and its affiliates have evolved, each terrorist cell tends to perform single functions, such as fund-raising or procurement. This compartmentalization of functions is clearly designed to protect the terrorist network against misadventure or exposure on the part of individual operatives. This beehive of decentralized and compartmentalized cells creates a network architecture that is all the

---

8 United Kingdom court translation of the *Encyclopedia of the Afghan Jihad*, accessible at URL: http://www.thesmokinggun.com/archive/jihadmanual.html, p. 10. *2004-2005*), p. 2.

more opaque and problematic for the authorities to monitor and take down. Nevertheless, an analysis of the functional activities occurring at each stage of the terrorism cycle can reveal its points of vulnerability to coordinated, calibrated counter-terrorist interventions.

Strategic Planning: Contemporary terrorist movements have demonstrated a capacity for skilful strategic planning for achieving tactical surprise. Available evidence indicates that strategic planning by terrorist groups can become a quite protracted process, taking months and even years of preparatory work prior to an assault. Often planners will move about, meeting in different cities and even countries, to lessen the risk of premature detection. This appears to have been the case with regard to the terrorist bombing of Air India flight 182, the September 11 attacks on the United States, the 2005 assaults on the London transit system, among other terror strikes. Indeed, as the US 9/11 Commission noted, travel is of no less importance for terrorists as are weapons.[9]

Al-Qaeda strategic planning reflects a long-term, centrally directed, high-level pursuit of Jihadist goals, notwithstanding the devolution of operational command and control to decentralized cells. Al-Qaeda strategizing appears to involve a three tier process: the proclamation of Jihadist strategy, tactical planning, and preparation of plans of attack. Jihadist strategy is the domain of top-echelon leaders, primary among them Osama bin Laden, who provide theological dispensation, political justification and warning about their intended course of religious struggle. A 2004 'summit' convened in a remote village in the remote northwestern Pakistani district of Waziristan reportedly served to formulate and communicate al-Qaeda's updated strategic doctrine to operational planners.[10]

Recruitment: The recruitment of activists and operatives is a prerequisite for the existence and continuity of any terrorist group. A Danish Ministry of Justice report on *Recruitment of Islamicist Terrorists in Europe* describes "Recruitment (as) the bridge between a personal belief and violent activism."[11] Some are recruited as activists to perform the various upkeep

---

9 The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Report* (New York: St. Martin's, 2004), p. 548.

10 Daniel McGrory and Michael Evans, "Net widens as al-Qaeda bomb link is confirmed." *The Times* [London], 15 July 2005

11 Michael Taarnby, *Recruitment of Islamic Terrorists in Europe. Trends and Perspectives*, Research Report Funded by the Danish Ministry of Justice, Centre for Cultural Research, University of Aarhus (Denmark), 14 January 2005, p. 6.

functions necessary for the continued viability of the terror organization, such as fund-raising, logistics, and communications. Others are recruited as operatives for training and deployment to actually undertake terror attacks, including suicide-bombings. Terrorist recruitment actively occurs also in Canadian communities.[12]

Since terrorist organizations operate illicitly they cannot recruit openly and publicly. Recruitment to terror organizations is itself a clandestine activity. Recent indications are that much of the recruitment al-Qaeda and its affiliates in the Muslim diaspora now involve self-enlistment. Individuals join through friendship or kinship ties, often under the inspiration of local religious preachers or teachers.[13] Much of the subsequent radicalization is fostered through the Internet, where a plethora of Jihadist websites foment a religious culture of militancy.

Notwithstanding this self-recruitment syndrome, there is evidence that al-Qaeda and its affiliates assign agent handlers to exercise oversight and even verification of recruitment and recruits, and to enforce discipline and militate against penetration.[14] Talent spotters are dispatched to appropriate venues, whether university clubs, communal associations or religious circles, to identify likely candidates for recruitment.[15] Universities have been targeted by al-Qaeda and other international terrorist groups as especially appropriate places to talent-spot and recruit educated cadres.[16] Even in a placid country like Norway, where there is but a minimal multicultural presence, the head of that country's Police Security Service *(Politiets sikkerhetstjeneste - PST)*, its intelligence and security agency, recently noted publicly for the first time that extremist Jihadists are busy recruiting local Muslim youth to carry out terrorist attacks and holy war.[17]

---

12 Clerk of the Privy Council, Intelligence Brief for the Prime Minister, *Radicalization and Jihad in the West*, prepared by the Canadian Security Intelligence Service, S-15(1), 7 June 2006; CSIS, *Public Report*

13 *Vide.* Arnaud de Borchgrave, Thomas Sanderson, Jacqueline Harned, *Force Multiplier for Intelligence*, A Report of the Transnational Threats Project, Center for Strategic and International Studies (Washington, DC: Centre for Strategic and International Studies, 2007), p. 13.

14 Rohan Gunaratna, *Inside Al Qaeda* (New York: Berkeley, 2002), p. 77; Taarnby, *Recruitment of Islamist Terrorists in Europe*

15 Daniel McGrory & Zahid Hussain, "New wave of British terrorists are taught at schools, not in the mountains," *The Times* [London], 14 July 2005; Stewart Bell, "Authorities wary of 'homegrown' terrorists: The next generation: Recruiting locals allows extremists to thwart security," *National Post* [Toronto] 14 July 2005.

16 UK Department for Innovation, Universities and Skills, *Promoting Good Campus Relations, Fostering Shared Values and Preventing Violent Extremism in Universities and Higher Education Colleges (London,* January, 2008), esp. Annex A: "Al-Qa'ida Influenced Violent Extremism and the Recruitment and Grooming Process Used by Violent Extremist Groups," p. 20; Anthony Bergin & Raspal Khosa, *Australian Universities and Terrorism*, Australian Strategic Policy Institute, Policy Paper #8, 2007.

17 "Extremists target local youth," *Aftenposten* [Oslo], 6 February 2008

As well, radical Islamist clerics in various countries across the world, from Britain and France to Australia, have been active in visiting prisons, promoting conversion and instilling extremist beliefs among inmates.[18] After release, ex-convict converts have been subsequently channeled to radical mosques where they are prone to virulent preaching and recruitment by militant elements.

Security authorities claim that al-Qaeda and its affiliates are deliberately "refocusing [their] efforts" to recruit youths of American, Canadian, or European background in their ranks.[19] These 'clean skin' (so-called) recruits are considered better able pass undetected through surveillance and border controls. They would also provide better camouflaged for clandestine operations against targeted countries. An up-to-date assessment by the United States Director of National Intelligence notes the al-Qaeda recruitment of Westerners capable of blending into American society and attacking domestic targets.[20]

As for the recruits themselves, an assessment of known al-Qaeda perpetrators indicates the following attributes pertaining to contemporary militant Jihadists[21]:

- Most militant Jihadists today are based in the Muslim diaspora, predominantly in Western Europe and North America. Most are engaged in the jihad outside their countries of origin, and indeed a growing number are second- or even third-generation diaspora born and/or educated.

- The preferred cell size seems to be 8 members, often composed of friends made during the formative ages of 15-30. Family bonds tend to predominant before age 15.

---

18 Jamie Doward and Anushka Asthana, "Al-Qaeda threat to British prisons," *The Observer* [London], 10 February 2008; John Rosenthal , "The French Path to Jihad," *Policy Review*, No. 139 (2006); Richard Ford, "Jail 'helps to radicalise Muslims'," *The Times* [London], 13 April 2007; Jamie Doward, "Terror training in prisons as al-Qaeda targets young," *The Observer* [London], 15 July 2007; Richard Kerbaj, "Radicals brainwashing Aborigines in prison," *The Australian* [Sydney], 17 August 2006.

19 Elaine Shannon, "Al-Qaeda Seeks Canadian Operatives to get around Tighter U.S. Security. Osama Bin Laden is Trying to Recruit Disaffected Muslims North of the Border," *Time Magazine*, 8 July 2003.

20 J. Michael McConnell, Director of National Intelligence, *Annual Threat Assessment by the Director of National Intelligence for the Senate Select Committee on Intelligence, 5 February 2008* (Washington, 2008). See also Mark Mazzetti, "Intelligence Chief Cites Qaeda Threat to U.S." *New York Times*, 6 February 2008.

21 Vide. de Borchgrave, et al, Force Multiplier for Intelligence, pp. 13-14.

- Most Jihadists are married, and fulfill their family responsibilities. Women tend to play an important role in promoting the small-group dynamics of the cell.

- The majority of Jihadists, and a plurality of suicide bombers, are well educated, and have university degrees or advanced technical training (except for European militants of Maghrebi descent, and suicide bombers in Iraq). The predominant profession represented among Jihadists is engineering. Computer science is another well represented professional discipline among educated Jihadists. Most members of cells have no criminal record, and they are often better off economically and socially than the neighbouring population.

- A common trait amongst Jihadist militants and leaders in the diaspora is their prior involvement in vigorous action-oriented group activities such as soccer, cricket, and other sports.

Training: Training prepares recruits to become terrorist activists and operatives. The skills and knowledge proficiencies sought by contemporary terrorist organizations covers a wide spectrum of learning, from flying aircraft to computer technology, biological and chemical sciences, to finance; from the preparation of explosives and explosive devises to actual combat. During the period of Taliban rule over Afghanistan some 70,000 Jihadist recruits traveled to that country from around the world for military training in camps run by al-Qaeda.[22] Since then, militant Jihadists have sought alternative venues for training, whether at secret facilities in congenial countries like Iran, Lebanon, Sudan or Pakistan, in combat zones in Chechnya or Bosnia, or at insurgent bases in Iraq.[23] There were even in training facilities set up in remote locations in Britain, Canada, Europe and the United States, and urban training camps in safe houses in British and European and also Canadian cities wherein al-Qaeda instructors imparted mission-specific skills relating to weaponry, explosives, and tactics.[24] In recent years terrorist recruits from Europe, the Middle East, Southeast Asia, Australia and North America have journeyed to Pakistan for operational training in al-Qaeda camps in that country.[25]

---

22 "Al-Qaeda camps 'trained 70,000'", *BBC News* http://news.bbc.co.uk/2/hi/europe/4146969.stm.

23 McGrory & Hussain, "New wave of British terrorists are taught at schools, not in the mountains"; Dana Priest & Josh White, "War Helps Recruit Terrorists, Hill Told," *Washington Post*, 17 February 2005.

24 Rohan Gunaratna, *Inside Al Qaeda. Global Network of Terror* (New York: Berkeley, 2002), p. 111.

25 Dirk Laabs and Sebastian Rotella, "Terrorists in training head to Pakistan
A dangerous new pattern emerges, illustrated by cases in Denmark and Germany," *Los Angeles Times*, 14 October 2007. 2 (2008).

Communications: Terrorist networks, cells, and their auxiliaries and front organizations rely on communications for the sinews that bind them together, to facilitate coordination and information sharing amongst individual components of the terror apparatus, to disseminate strategic, tactical and operational information about targets, objectives, and goals; and to deliver operational instructions. The Internet plays a key role in terrorist communications by e-mail (best encrypted) and through open-access and password-guarded websites. Al-Qaeda places high priority on secure communications, and its operational guidelines insist that communicating should be concise, secret and pertinent.[26] Being aware of the vulnerability of postal and electronic systems to interception, however, terror groups tend to entrust their most sensitive communications to reliable, dedicated couriers to convey face -to-face to far flung branches of their networks.[27] These couriers may sometimes carry physical messages, whether letters, audio cassettes or videos, but often the secret messages are entrusted solely to memory.[28]

Resourcing: Al-Qaeda, its affiliates, and other Jihadist terror groups engage in systematic fund-raising and money-laundering to finance their widespread system of networks, cells, affiliates and auxiliaries, and their related activities.[29] Significant monies also go to pay for the terrorist propensity to travel around the world.[30] Terrorist organizations typically raise funds by soliciting private donations, by diverting revenues from quasi-legitimate businesses, Non-Governmental Organizations and fronts, and through criminal activities. Militant Islamicist groups try to exploit the charitable injunctions of Islam to elicit donations directly or through religious institutions or sympathetic ethno-cultural organizations.[31] Al-Qaeda is known to have set up charitable fronts, such as the Benevolence International Fund, to raise and transfer money to

---

26 Guneratna, *Inside Al Qaeda*, pp. 108-9.

27 Gunaratna, *Inside Al Qaeda*, p. 108.

28 Robert Fisk, "With Runners and Whispers, al-Qa'ida Outfoxes US Forces," *The Independent* [London], 6 December 2002.

29 Martin Rudner, "Using Financial Intelligence Against the Funding of Terrorism, "*International Journal of Intelligence and CounterIntelligence*, Vol. 19, No.1 (2006). See also International Monetary Fund, Legal Department, *Suppressing the Financing of Terrorism: A Handbook for Legislative Drafting* (Washington, DC: International Monetary Fund, 2003), and Stewart Bell, "Blood Money: International Terrorist Fundraising in Canada," in Norman Hillmer and Maureen Appel Molot, eds., *Canada Among Nations 2002. A Fading Power* (Toronto: Oxford University Press, 2002).

30 US National Counterterrorism Center, *National Strategy to Combat Terrorist Travel* (NCTC National Counterterrorism Center, May 2, 2006), p. 17. See also Martin Rudner, "Misuse of Passports: Identity Fraud, the Propensity to Travel, and International Terrorism," *Studies in Conflict and Terrorism*, Vol. 31, No.

31 Matthew Levitt, *Charitable Organizations and Terrorist Financing: A War on Terror Status-Check*, Paper presented at "The Dimensions of Terrorist Financing", University of Pittsburgh, March 19-20, 2004; Daniel Pipes, "U.S. Court Blows Terrorists' Cover," *Chicago Sun-Times*, 15 December 2004.

finance terrorist activities. According to the Norwegian Defence Research Establishment report on *Jihad in Europe*, mosques in Germany, France, the UK and elsewhere were "hijacked" by radical elements to be used for fund-raising, recruitment, incitement and propaganda, and even for preparing terrorist assaults.[32] Militant groups have also raised substantial funds through the sale of inspirational tracts, advocacy literature, audio cassettes, videos and CDs, and other iconic paraphernalia.[33]

Terrorist organizations have also engaged in criminal activities to augment their fund-raising. The Moroccan-dominated *al-Qaeda* cells that perpetrated the March, 2004 terror attacks on Madrid commuter trains were funded by bank robberies in Spain and sophisticated ATM fraud in France.[34] In January, 2005, German police in five states raided premises and arrested 14 suspects belonging to a criminal Islamicist organization allegedly involved in smuggling, document forgery, recruitment of militants, Jihadist incitement and terrorism finance.[35]

Among the criminal activities attributed to international terrorist groups are the sale of fraudulent passports and identity documents, people smuggling, credit card fraud, drug trafficking, trade in contraband, and automobile theft and re-export.[36]

Terrorist resourcing remits substantial funds through financial systems, including informal *hawalas*, to wherever these organizations seek their deposit or use.[37] It is noteworthy as well that certain high-value, compressed forms of wealth, like diamonds, narcotics or other contraband are usually shipped with trusted couriers surreptitiously to their intended destinations.[38]

Procurement: The procurement by terrorist organizations of matèriel needed for their operations includes acquiring weapons, explosives,

---

32 Netter, *Jihad in Europe*, p. 50. See also Vidino, *Al Qaeda in Europe*, pp. 89-94.

33 *Cf.* Thomas Friedman, "Giving the Hatemongers No Place to Hide," *New York Times*, 22 July 2005.

34 Damien McElroy, "Cashpoint Fraud Funded Terror Attacks in Spain," *Daily Telegraph* [London], 4 November 2004.

35 "German Police Arrest Suspected Islamic Extremists," *Washington* Post, 12 January 2005.

36 Stewart Bell, *Cold Terror. How Canada Nurtures and Exports Terrorism Around the World* (Toronto: Wiley, 2004), pp. 197; Timothy Appleby, "Scam allegedly funnelled cash to Tamil Tigers, *Globe and Mail* [Toronto], 31 January 2008.

37 On terrorism finance see Rudner, "Using Financial Intelligence Against the Funding of Terrorism"; J. Millard Burr & Robert Collins, *Alms for Jihad* (Cambridge University Press, 2006).

38 Douglas Farah, *Blood From Stones: The Secret Financial Network of Terror* (Broadway Books, 2004); *For a Few Dollars More. How al Qaeda Moved into the Diamond Trade*, Global Witness (April, 2003).

vehicles, fraudulent passports, other equipment and supplies. Lacking a conventional industrial base of their own, terror groups are obliged to acquire this matèriel from other legitimate sources by stealth or by theft. An intercepted al-Qaeda communication cited by the Italian Divisioni Investigazioni Generali e Operazioni Speciali (DIGOS - Division for General Investigations and Special Operations) highlighted the role of logistical elements in the following terms:

> "...if the brothers want to hide, we hide them, if the brothers want documents, we take care of these documents, if the brothers want to move, we move them... if they need a weapon, you give them a weapon..."[39]

Sometimes the matèriel can be surreptitiously acquired whole. In 2005 and 2006 a UK-based Islamist terror cell shipped freight-loads of equipment to terrorist contacts in Pakistan, under the guise of assistance for earthquake victims.[40] Otherwise, terror groups have tended to procure the raw materials – the better to disguise their intentions – with which to fabricate by themselves the desired explosives or weapons. Thus, Jihadist groups in Belgium, Britain Italy, and Spain were caught with chemicals for producing explosives and chemical agents.[41]

One of the more alarming aspects of international terrorism is the evidence that al-Qaeda and other Jihadist groups are attempting to acquire chemical, biological, radiological and nuclear (CBRN) attack capabilities.[42] In a June 2002 article, al-Qaeda spokesman Sulaiman Abu Gaith insisted "it is our right to fight [the Americans] with chemical and biological weapons."[43] Jihadist groups in Belgium, Britain Italy, and Spain have been discovered with ingredients for producing explosives and chemical agents.[44] There is suspicion that terrorists will try to enroll operatives in universities and research institutes in advanced industrialized countries in order to avail themselves of training and laboratory work in sensitive, dual-use subjects like nuclear science, computer engineering, which could have terrorist applications.[45]

---

39 DIGOS, *Report al Mhajoroun 1* (Milan, 2 April 2001), cited in Vidino, *Al Qaeda in Europe*, p. 77.
40 David Byers, "Gang plotted to behead Muslim soldier 'like a pig'," *The Times* [London], 29 January 2008.
41 "Suspicious Attempts Made to Buy Bomb Materials," *Globe and Mail* [Toronto], 6 January 2005.
42 Canadian Security Intelligence Service, *Public Report 2003* (Ottawa, 2003), pp. 2, 5.
43 MI-5 The Security Service, *The Threats*. http://www.mi5.gov.uk/output/Page25.html
44 "Suspicious Attempts Made to Buy Bomb Materials," *Globe and Mail*.
45 Francis Elliot, "Universities Unwittingly Training 'Kitchen Sink' Terrorists," *Daily Telegraph* [London], 13 January 2003; "Science and National Security," *Washington Times*, 22 January 2003.

Infrastructure: International terror networks require an infrastructure of safe houses and sleeper cells to accommodate and service operatives on current missions, and to sustain a covert capacity for future operations. International terrorist networks typically maintain chains of safe houses in various cities and countries across the world, relocating among them at the various stages of operational planning, so as to minimize risks of discovery.[46] Sometimes the safe houses are kept dormant, or are used by unassociated third-parties, until required for operations. Sleeper cells comprise terrorist units that are kept inactive, sometimes for extensive periods of time, even years.[47] This is to enable them to escape surveillance by counter-terrorism authorities while remaining in readiness for reactivation for future missions.[48]

Propaganda: International terrorist networks typically utilize front organizations to transmit their propaganda and incite militant action. The former imam of the Finsbury Mosque in London, Sheikh Abu Hamza, was convicted in February, 2006 under Britain's Anti-Terrorism, Crime and Security Act, 2001, for soliciting the murders of Jews and non-believers and for provoking racial hatred.[49] Another British Islamist extremist, Abdullah e-Faisal, was sentenced in 2003 to nine-years imprisonment for "inciting racial hatred and incitement to murder."[50] A terror network in Germany based in mosques in various cities used to spread militant Islamic propaganda that summoned recruits to join a Jihad against the West.[51] Some groups also sponsor circuits of traveling clerics and itinerant activist-agitators who pass through local communities to radicalize the faithful and galvanize support among followers for the militant enterprise. Indoctrinated adherents would then be encouraged to go abroad to training camps to acquire terrorist skills for operations as *mujahideen*.

Terrorist propaganda and incitement against perceived enemies are intended to justify militant activities and cultivate followers and sympathizers. The goals are to mobilize broad based backing and commitment from within the religio-ethnic community and attract

---

46 US Department of State US Department of State, Office of the Coordinator for Counterterorism, *Country Reports on Terrorism 2005* (Washington, DC: 2006), p. 17.

47 Gunaratna, *Inside Al Qaeda*, pp. 105-6.

48 Vidino, *Al Qaeda in* Europe, pp. 78-79; Gunaratna, *Al Qaeda*, pp. 105-6.

49 Sean O'Neill and Daniel McGrory, "Kill and be killed: how cleric raised generation of terrorists," *The Times* [London], 8 February 2006.

50 US Department of State, *Patterns of Global Terrorism 2003*, p. 57.

51 Tony Paterson, "Raids on Mosques Broke Terror Network, Claim German Police in Berlin," *The Independent* [London], 13 January 2005.

prospective recruits to the movement.[52] Some links in the al-Qaeda propaganda chain are known to have been located in Canada. Among these were nodes belonging to the so-called Global Islamic Media Front preparing Jihadist incitement materials for dissemination across North America, Europe and the world.[53] Militant Jihadist agitprop tends to foment domestic radicalization in countries like Canada, stirring up enmity from within whilst creating an environment that encourages terrorist recruitment and activism.[54] Terrorist elements in Canada have used front organizations for advocacy purposes, and have also coerced and manipulated local homeland communities to conform and lend support to the militant agenda.[55] Within certain communities militant elements have subverted and taken over religious and ethno-cultural institutions and Non-Governmental Organizations, turning them into bastions for the militant cause. Moderates were effectively marginalized, manipulated and coerced into compliance.

Al-Qaeda has established its own intelligence capacity for ***penetrating sensitive government departments, agencies and institutions*** with agents, including sleeper agents, double agents, agents provocateurs, recruit insiders ("moles"), and fifth columnists.[56] Their objectives include:

- Infiltrating National Security secrecy to collect sensitive information and plans
- Detecting and disrupting National Security operations
- Acquiring sensitive technologies
- Strategic deception to confound the targeted organization's situational awareness
- The manipulation and distortion of public opinion in the battle for minds

---

52 On the activities and doctrines propagated by radical Islamicist groups of various stripes see Olivier Roy, *Globalised Islam. The Search for a New Ummah* (London: Hurst & Co., 2004), pp.234-257; see also Vidino, *Al Qaeda in Europe*, esp. Chap. 1.

53 Graeme Hamilton, "Al-Qaeda's 'Spokesman'," *National Post* [Toronto], 1 February 2008.

54 Canadian Security Intelligence Service, *The Radicalizers: The Islamist Extremist Threat to Canada from Within*, Study 2006-7/09(a), 15 Dec 2006.

55 Canadian Security Intelligence Service, *Public Report 2003*, p. 4.

56 Brian Fishman, *Al-Qa'ida's Spymaster Analyzes the U.S. Intelligence Community* (West Point, NY: United States Military Academy, 2006).

Their tradecraft is said to be masterful. Targets for penetration include security and intelligence agencies, key government departments, sensitive industries, universities, human rights organizations, and the legal profession.[57] This espionage function is so important that Al-Qaeda operational doctrine treats infiltration into sensitive Government departments, agencies and institutions as the strategic equivalent of "martyrdom" attacks on the infidel enemy.[58]

Tactical preparations: Tactical preparations for terror attacks are usually vested in small, tightly knit cadres within operational cells. It is not usual for these cadres to counsel or seek advice on tactical operational details with other specially-qualified operatives in-country or even abroad. In a notorious case in the UK, known as Operation Crevice, the terror cell that conspired to attack gas and electricity plants in Britain sought technical input from an alleged co-conspirator in Canada.[59] Tactical preparations for terror operations may entail meetings of commanders and operatives staged at different times in various locations, even in different countries, in order to elude surveillance and detection. This tactical preparatory phase for major assaults can extend over many months and even years. The September 11th attackers engaged in prolonged tactical planning and preparations in various locations across the United States prior to embarking on their deadly mission.[60]

Reconnaissance on targets: Al-Qaeda and other Jihadist terror organizations usually undertake a careful, detailed and continuous reconnaissance on their intended targets. Successive reconnaissance teams may be brought to bear, along with specialized skills and methods, even accessing architectural drawings and infrastructure maps. Reconnaissance missions, with the support of local cells, aim to pinpoint target vulnerabilities, identify tactical approaches and escape routes, and guide tactical commanders and operatives in readiness for the assault.[61] Fraudulent identities can facilitate travel by reconnaissance missions and their surreptitious entry even to the most vigilant of target countries.

---

57 *Cf.* Lisa Kramer & Richards Heuer Jr., "America's Increased Vulnerability to Insider Espionage," *International Journal of Intelligence and CounterIntelligence*, Vol. 20, No. 1 (2007), pp. 50-64; Stephen Wright , "Revealed: Islamist extremists have penetrated the heart of Britain," *Daily Mail* [London][, 12 February 2008; Ben Leapman, "Al-Qaeda supporters working at strategic sites," *Sunday Telegraph* [London], 29 April 2007.

58 Abu Bakr Naji, *The Management of Savagery*, trans. William McCants, (West Point, NY: United States Military Academy, Combating Terrorism Centre, 2006), section 9.

59 Philippe Naughton, "Five given life for fertilizer bomb terror plot. Link to 7/7 bombers can be revealed for the first time," *The Times* (London), 30 April 2007.

60 *The 9/11 Report*, pp. 226-231.

61 Rohan Gunaratna & Peter Chalk, *Jane's Counter Terrorism, 2nd Edition* (Coulsdon, Surrey: Jane's Information Group, 2002), p. 52.

Although mounting such extensive reconnaissance does involve risks of discovery, the attention to detail is expected to enhance the likelihood of a successful attack, with maximum harm to the target.

Terrorist assaults: Terrorist assaults are characterized by stealth, surprise and ruthless ferocity. A wide repertoire of tactics may be used in mounting attacks on targets, from armed attacks using bombs, firearms, or missiles, to suicide bombings, ambushes, hostage taking, assassinations, and vehicle-weapons in cars, trucks, planes, ships, trains, etc. Recent attacks on Jakarta, London, Tel Aviv, Baghdad, Algiers, London, Madrid and elsewhere indicate that suicide-bombers and car/truck bombing are now becoming the terror tactics of choice.[62] Some attacks attributed to al-Qaeda or its affiliates against targets in Egypt, Great Britain, Indonesia, Morocco, Spain, Saudi Arabia, and Turkey involved primarily local, in-country cells and networks. However, it is not uncommon for Jihadist terrorists to assemble their strike force from various parts of their network, local and international. A Jihadist terror cell convicted in April, 2007, of plotting attacks on British targets, including a electricity and gas facilities, was composed of militants residing in the U.K. but also involved co-conspirators from the United States, Canada and Pakistan.[63]

4. POINTS OF VULNERABILITY TO COUNTER-TERRORISM INTERVENTIONS

In general, there are five sources and methods available to intelligence and security authorities to discern, detect and investigate terrorist intentions and capabilities:

- Planting and running agents in suspected terrorist cells and networks
- Acquiring "walk-ins," and/or recruiting "moles" as informants inside suspected terrorist cells and networks
- Deploying technical means to monitor activities of suspected terrorist cells and networks, utilizing communications, imagery, financial intelligence, and/or sensor technologies

---

62 *David R. Sands, "Reading minds of suicide bombers,"* Washington Times, *24 July 2005; Craig Whitlock, "Al Qaeda Leaders Seen in Control,"* Washington Post, *24 July 2005*

63 "Five Given Life for Fertiliser Bomb Terror Plot . Link to 7/7 Bombers can be Revealed for the First Time," *The Times* [London], 30 April 2007.

- Interrogating captured terrorist assets, including detained operatives, captured documents, seized computer hard-drives, and/or forensic analysis

- Liaison and intelligence sharing with the security, intelligence, and law enforcement agencies of allied and friendly countries.

Agent running, whether planted agents, "walk-ins" or "moles," and the interrogation of detained suspects, constitute so-called "Human-source" intelligence (HUMINT). In Canada, HUMINT generally falls within the jurisdiction of CSIS, RCMP, Canada Border Services Agency (CBSA) and other law enforcement agencies.[64] Certain of the technical means are the mandated responsibility of functionally specialized agencies, most notably the Communications Security Establishment (CSE) for communications and electronics intelligence collection, and the Financial Transactions and Reports Analysis Center of Canada (FINTRAC) for financial intelligence. However, these and other technical means of intelligence collection can also be deployed by CSIS, RCMP and other law enforcement agencies as provided by law. International liaison with allied and friendly countries has become an increasingly important source of shared intelligence in this age of globalized terrorist networks, yet any dependency on external sources can render our national security efforts vulnerable to the mishaps, manipulations, malfeasance or travesties of others.[65]

An examination of the terrorist operational cycle reveals certain points of vulnerability, potentially, to counter-terrorism interventions by intelligence, law enforcement and national security agencies to protect against threats of attack. These interventions entail a broad array of operational capabilities involving all the relevant security and intelligence disciplines: HUMINT -- collected by domestic, foreign and criminal intelligence organizations, SIGINT, imagery intelligence (IMINT), financial intelligence, border control, regulatory authorities, intelligence

---

64 Though somewhat dated by now, the publication of Canada's Privy Council Office, *The Canadian Security and Intelligence Community. Helping Keep Canada ad Canadians Safe and Secure* (Ottawa, 2001) offers a survey of the roles and responsibilities of various intelligence, security and law enforcement agencies. For a more recent academic study see Rudner, "Challenge and Response: Canada's Intelligence Community and the War on Terrorism."

65 *Cf.* Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National* Security *Activities* (Ottawa: Public Works and Government Services Canada, 2006), p.431-2. See international liaison and counter-terrorism see also Stéphane Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence*, Vol. 16, No. 4 (2003); Martin Rudner, "Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism," *International Journal of Intelligence and CounterIntelligence*, Vol. 17, No. 2 (2004); Jennifer E. Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," *International Journal of Intelligence and CounterIntelligence*, Vol. 19, No. 2, (2006)

analysis and threat assessment. Not all the postulated interventions are necessarily being pursued currently by the responsible agencies, however these interventions are presumed to be consistent with their respective mandates and appropriate to their operational roles.

Strategic Planning: The characteristic propensity of al-Qaeda and its affiliated networks to engage in extensive discourses about Islamic legal precepts regarding their strategic planning, including the issuance of *fatwas* (juridical permissions) for operations against specified targets, provides a window of insight into their planned intentions, tactical capabilities, and operational doctrines. Since this discourse and the ensuing *fatwas* must necessarily be shared with operatives, sympathizers and supporters, their communications by electronic or print media, or even orally through selected preachers and messengers, are inherently vulnerable to interception. Moreover, *Shariyah* (Islamic law) obliges Muslim warriors to issue warnings to targets of attack, which Jihadists often do. To be sure, these warnings may not always be cast in a form, language or terminology familiar to non-Muslims.

For security authorities to gain access to the high-level planning intentions of al-Qaeda and its affiliates would therefore require both a capacity to access their communications and the capability to analyze and interpret the embodied messages. Signals intelligence capabilities can be deployed to intercept and decipher Internet communications and also penetrate password-protected websites. Security intelligence may penetrate religious circles in order to collect human source information on extremist preaching. However, it will remain for intelligence assessment to contribute an understanding of the actual substance and implications of terrorist strategic planning and operational doctrines. Assessment of strategic intent could be further reinforced and enhanced by the commissioning of related research studies by experts in the academic and consulting communities to contextualize the militant Jihadist ideology and mindset so as to help discern the adversaries' purposes in advance.

Recruitment: Once there are reasonable grounds to suspect that particular groups are engaged in terrorist activities, they may be lawfully investigated and their activities monitored, also by infiltrating intelligence agents into their midst. A primary objective of the ensuing investigation should be to identity the membership of the suspected terrorist cell or network, including recent recruits. Along with this investigative effort, security intelligence services and law enforcement agencies may be

expected to also try to determine the scope and methodologies of terrorist talent-spotting and recruitment efforts. Moreover, the SIGINT monitoring of suspected terrorist websites should permit the tracking of prospective self-enlisting recruits to the militant Jihadist movement

Training: The security intelligence/law enforcement surveillance of suspected terrorist cells and networks would also be expected to detect and monitor their training activities. In so far as al-Qaeda networks resort to more advance training abroad, as they tend to do in camps in Pakistan, it would be for border controls to detect the movements of suspected trainees and trainers based on shared information from domestic and international intelligence sources.

Communications: Terrorist communications by Internet or telephone are vulnerable to lawful interception by security intelligence or law enforcement agencies, domestically under warrant, or by the SIGINT agencies internationally. To be sure, signals intelligence faces massive challenges, technologically and in quantum terms, in seeking to track and intercept terrorist communications. The ever increasing sophistication of communications technologies, coupled with the ready availability of highly capable information security applications, renders the SIGINT task considerably more intricate. Furthermore, the sheer volume of communications traffic makes the targeting of specific, suspect messages very demanding. Nevertheless, SIGINT has come to play a vital role in counter-terrorism, with international SIGINT alliances and partnerships providing mechanisms for burden sharing and information sharing.[66] For its part, the terrorist network's use of couriers for the inter-personal transmission of message is itself vulnerable to detection through the intelligence/law enforcement surveillance of local suspected networks and cells, reinforced by border controls.

Resourcing: Terrorism financing, fund-raising and money transfers are vulnerable to scrutiny and tracking on the part of specialized financial intelligence units, like FINTRAC, as well as by security intelligence and law enforcement agencies. Government revenue agencies can vet charitable organizations, including religious institutions, to counteract the inappropriate use of charitable donations. Border controls may be applied to prevent the illicit importation of undeclared monetary instruments.

---

66 *Vide.* Martin Rudner, "Canada's Communications Security Establishment, Signals Intelligence and Counter-Terrorism," *Intelligence and National Security*, Vol. 22, No. 4 (2007).

Procurement: The procurement by terrorist elements of supplies and materiel is difficult to track and control in open, democratic societies, except where the transaction actually involves a legal transgression. Alas, much of what terrorists wish to procure for their operations may be acquired lawfully, even explosives. In these circumstances, in most democracies it falls to several key regulatory authorities and law enforcement agencies to try to counteract the unlawful acquisition of materiel and supplies for terrorist purposes. Thus, for example, Natural Resources Canada has regulatory authority over explosives, and Passport Canada over the issuance of passports, while the Canadian Border Service Agency is responsible for border controls and for monitoring the import of dangerous cargoes. It was an alert British port official who detected members of the UK cell with a shopping list of sophisticated equipment sought by terrorist contacts in Pakistan.[67]

Infrastructure: The terrorist infrastructure of safe houses and sleeper cells is deliberately designed to withstand detection and surveillance in order to remain available for future operations. A well-ensconced network of safe houses and sleeper cells can be very hard for the authorities to unravel. Patient, careful, sustained intelligence and police work over a prolonged time frame would be required to uncover most or all of these clandestine terrorist infrastructures.

Propaganda: Terrorist incitement, propaganda and indoctrination efforts typically make use of the Internet and the preachings of radical clerics to convey their belligerent messages. These media can be and often are followed by the authorities, through communications intelligence, security intelligence, or criminal intelligence/law enforcement, and also by non-governmental research organizations. Thus, the Global Islamic Media Front, including suspected propagandists based in Canada, was reportedly detected and interrupted by Austrian SIGINT authorities, which shared the evidence with Canadian counterparts.[68] Sometimes the messaging conveyed by al-Qaeda and other militant Jihadist pronouncements will allude to intended actions or targets, so as to gainsay religious jurisprudential sanction for future operations.[69] Their agitprop, therefore, demands serious attention. Often, however, the messaging is conveyed in obscure, nuanced terminology or allusions to Islamic phenomena

---

67 David Byers, "Gang plotted to behead Muslim soldier 'like a pig'," *The Times* [London], 29 January 2008.
68 Hamilton, "Al-Qaeda's 'Spokesman'", p. A1.
69 Netherlands General Intelligence and Security Service (AIVD), *The Radical Dawa in Transition* (The Hague: Ministry of the Interior and Kingdom Relations, 2007), p. 11 *et passim*

unfamiliar to the uninitiated. These pronouncements must therefore be subject to careful, ongoing analysis and assessment by knowledgeable experts in order to fully appreciate the ideological significance and operational implications of the militant Jihadist propaganda effort.

Penetration: Terrorist infiltrations into government departments, security and intelligence agencies, sensitive industries, or civil society organizations can create an insider threat that can effectively undermine the overall capacity of democracies to defend themselves. This insider threat derives from the insidious exploitation and manipulation of human susceptibilities to betray institutional vulnerabilities. These terrorist attempts at insider espionage are themselves vulnerable to the classic counter-intelligence approaches to detecting penetrations:[70]

- Anomalies and Inconsistencies approach
- Litmus Test approach
- Motive approach
- Cost Accounting approach
- Predictive Test approach

To protect against terrorist penetration efforts and insider threats, counter-intelligence disciplines must be enlisted in counter-terrorism. Thus, by virtue of vigilance, the UK Security Service is reported to have detected and thwarted "dozens" of al-Qaeda attempts to infiltrate its ranks during its recent surge in recruitment.[71]

Tactical preparations: The tendency of terrorist networks to assign tactical preparations to small, tightly-knit groups of operational cadres makes it difficult for intelligence or law enforcement agencies to penetrate into their terror planning initiatives with informants, even if the cell is itself under surveillance. Nevertheless, terrorist communications with co-conspirators and leaders in Pakistan are more likely to be vulnerable to interception, while the international movements of key planners and

---

70 Kramer & Heuer, "America's Increased Vulnerability to Insider Espionage," pp. 50-64.
71 "Al Qaeda Fanatics in Bid to Join MI5," *Daily Express* [London], 8 May 2007.

their co-conspirators may be monitored by border controls. Details of actual tactical plans may be more problematic for intelligence agencies to discern, without having successfully placed a human source within the cadre clique. Be that as it may, the propensity of terror tacticians to commit their operational plans and to computer hard-drives has tended to make them accessible to the authorities during the course of a subsequent investigation.

Reconnaissance: The terrorist propensity to undertake detailed reconnaissance of prospective targets exposes them to certain points of vulnerability. Terrorist operatives embarking on reconnaissance missions must to some extent make themselves and their intentions liable to discovery as they reconnoiter their indicated target. In the case of a group already under surveillance, a reconnaissance mission should well be treated by intelligence or law enforcement agencies as an early warning signal. Reconnaissance represents, indeed, a pre-indicator of intention to attack. Where critical national infrastructure is being targeted, a vigilant regimen for protective security on the part of owner/operators should be alert to any attempt at reconnaissance.

Terrorist Assault: A terrorist assault comprises the most perilous phase of the terrorism cycle. To be sure, a terrorist attack can possibly be interdicted in the course of the operation by the authorities, if advance warning is available. Otherwise, by the time a terrorist squad or explosives-laden vehicle arrives at the target site the immediately relevant response shifts from prevention to mitigation, so as to try to limit the potential casualties and mitigate the damage. Guards, gates, emergency preparations and resilience planning catapult to the forefront of the counter-terrorism intervention. In the aftermath of a terrorist strike, advance planning for managing consequential damage, emergency repairs, and resilience represent the ultimate security antidote to the worst efforts of terrorists to harm our core national interests

An overall matrix portraying intelligence-led interventions in the terrorism cycle citing Canadian Security and Intelligence capabilities is outlined in Table 1:

Table 1
INTELLIGENCE-LED INTERVENTIONS IN THE TERRORISM CYCLE

Terrorism Cycle Phase	CSIS	RCMP	Other Support	Key Discipline
Strategic Planning	X		CSE, IAS, ITAC	Analysis
Recruitment	X	X		HUMINT
Training	X	X	CBSA	HUMINT, BORDER CONTROL
Communications		X	CSE, CBSA	SIGINT, BORDER CONTROL
Resourcing	X	X	FINTRAC, CRA, CBSA	FININT, BORDER CONTROL
Propaganda/ Incitement	X	X	CSE	HUMINT, SIGINT
Infrastructure	X	X		HUMINT
Tactical Planning	X	X	CSE	HUMINT, SIGINT
Reconnaissance	X	X		HUMINT, IMINT
Assault		X	LOCAL GUARDS	HUMINT, CONSEQUENCE MANAGEMENT
Penetration	X	X	Security Officers	Counter-Intelligence

Key: *Agencies*: CSIS: Canadian Security Intelligence Service; RCMP: Royal Canadian Mounted Police; CSE: Communications Security Establishment; CBSA: Canadian Border Service Agency; FINTRAC: Financial Transactions and Reports Analysis Center of Canada; ITAC: Integrated Threat Assessment Centre; IAS: International Assessments Staff, Privy Council Office.

Disciplines: HUMINT: Human Source Intelligence; SIGINT: Signals Intelligence; FININT: Financial Intelligence; IMINT: Imagery or visual Intelligence.

5. TOWARDS ANALYSIS DRIVEN INTELLIGENCE

The traditional, primary role of intelligence analysis in the Canadian S&I Community has been to draw on the results of domestic intelligence collection coupled with shared information from allies in order to produce assessment products for dissemination to interested clients across government. Over time, Canada has evolved a complex web of multiple, centralized and decentralized intelligence assessment units, most of them relatively small in size -- the largest have 30-40 staff, except for Defence Intelligence which is far larger --- and having mixed mandates for producing strategic, tactical and operational intelligence analyses.

Most components of Canada's S&I community possess their own intelligence analysis capabilities. This is certainly not inappropriate, as it meets their respective requirements for analytical products germane to their mandates and missions. Thus, CSIS has its Intelligence Assessments Branch, the RCMP its Criminal Analysis Branch, FINTRAC its internal analytical resources, the Canadian Forces Defence Intelligence (J2), and law enforcement across the country have access to Criminal Intelligence Service Canada as well as their local analytical units. As well, other security-related departments and agencies also possessed their own capacity for analyzing internally-generated intelligence inputs, including the Canada Border Services Agency, Canada Revenue Agency, Citizenship and Immigration Canada, Department of Foreign Affairs and International Trade, Department of National Defence (Directorate of Strategic Analysis –D Strat-A), Department of Public Safety, Department of Transport, and Natural Resources Canada. Two high-level organs have been created to provide all-source strategic intelligence assessments for government clients. The central agency of government, the Privy Council Office has its International Assessment Staff (formerly known as the Intelligence Assessment Secretariat) producing intelligence assessments for Cabinet and inter-departmental policy-makers. In 2004, the Integrated Threat Assessment Centre (ITAC) was established as a national fusion centre for all-source intelligence assessments relating to terrorism and counter-terrorism for all levels of government, intelligence and law enforcement agencies, and first responders.

In this complex institutional context characteristic of the Canadian S&I Community the intelligence analysis function tends to be driven by

intelligence collection. Accordingly, their analytical production by and large consists of interpretations, syntheses and assessments relating to the perceived threat environment, strategic and tactical, for policy makers and managers. This form of analysis would not usually serve to directly support ongoing national security operations or investigations. In the Canadian S&I Community, intelligence analysis rarely, if ever, drives intelligence collection.

This traditional paradigm of intelligence analysis contrasts sharply with the more contemporary, integrative, actionable role assigned to intelligence analysis in the reports of the U.S. 9/11 Commission, the British Butler Committee, and Australia's Flood Inquiry. The new approach was reflected in the creation of so-called "fusion" centres as a centralized, integrative mechanism for all-source intelligence assessments.[72] The U.S. National Counterterrorism Center, the British Joint Terrorism Analysis Centre (JTAC), the Australian National Threat Assessment Centre, and, indeed, Canada's Integrated Threat Assessment Centre (ITAC) represent prominent examples of this centralized, integrative, "fusion" function in intelligence analysis. While these fusion centres might continue to produce intelligence assessments for policy makers and the political leadership, their distinct and innovative role would be to contribute all-source, actionable analysis to support proactive operational interventions against terrorist threats. The conceptual foundation has been laid, and it remains to be seen whether policy leadership and appropriate resourcing will eventually succeed in transforming intelligence analysis into operationally relevant and actionable prescriptions for intelligence-led interventions in terrorism cycle.[73]

A counter-terrorism strategy aimed at preemptive interventions in the terrorism cycle must be grounded on reliable, all-source, well-crafted and actionable intelligence analysis. The analysis function should be expected to produce operationally-relevant assessments of terrorist activities, in their detail, apropos each stage of the terrorism cycle as it pertains to targeted groups. These assessments would be fed back to intelligence and law enforcement agencies as prescriptions for further investigative operations, signaling where lacunae exist in available information.

---

72 *Vide.* Martin Rudner, "Intelligence Analysis and Counter-Terrorism: How Lies the Landscape?" in Magnus Ranstorp, ed., *Mapping Terrorism Research,* Studies in Intelligence series (London: Routledge, 2007); Stéphane Lefebvre, "A Look at Intelligence Analysis," *International Journal of Intelligence and CounterIntelligence*, Vol. 17, No. 2 (2004).

73 *Vide.* Mark Lowenthal, "Intelligence Analysis: Management and Transformation Issues," in Jennifer Sims & Burton L. Gerber, eds., *Transforming U.S. Intelligence.*

Already in the UK, the JTAC role encompasses the preparation both of strategic-level assessments for policy-makers and government leaders, and actionable analyses in direct support for Security Service (MI-5) and Secret Intelligence Service (MI-6) counter-terrorism operations.

Compared to the traditional approach which in analysis represented the trailing edge of collection, in this new paradigm intelligence analysis emerges as a driver of intelligence collection. A coordinating mechanism, to be discussed below, would orchestrate the ensuing efforts on the part of the agencies concerned to conduct their investigations and share information so as to fill in the missing gaps and thereby complete the intelligence picture. Whereas the intelligence disciplines, like HUMINT, SIGINT, and financial intelligence can paint the details, intelligence analysis projects the big picture.

For intelligence analysis to take on and fulfill this expanded, prescriptive role will require some far-reaching capacity building in the Canadian S&I Community. Three major issues will need to be addressed: (a) the institutional locus for an expanded, prescriptive intelligence analysis capability; (b) the professionalization of intelligence analysis in the Canadian S&I context; and, related to this, (c) the training and professional development requirements for enhanced intelligence analysts. Currently in Canada, even high-level strategic intelligence analysis is decentralized and fragmented among multiple organizations, ITAC, IAS, CSIS, D Strat-A, with sub-optimal staffing levels; except at DND. In most of these organizations the analysis function is performed mainly by officials seconded from other duties, and very few are actually career analysts. Moreover, training opportunities for intelligence analysts in the Canadian S&I Community are limited to barely rudimentary offerings at the elementary, entry level.

In these circumstances, there would seem to be distinct locational and operational advantages to relocating the national intelligence assessment fusion centre to the Privy Council Office through a merger of ITAC with IAS. A merged ITAC-IAS would create the critical mass, in terms of staffing and coverage, for building a more robust, more synergetic, more comprehensive and higher profile intelligence fusion centre at the central agency of the Government of Canada. It is noteworthy, in this regard, that the United States and Australia both locate their high-level intelligence assessment organs in their respective central agencies, the US National Counterterrorism Center in the Office of the Director of

National Intelligence, and the Australian Office of National Assessment in the Department of the Prime Minister and Cabinet. Such a merged ITAC-IAS fusion centre could expand the capacity for intelligence analysis in Canada, while its identification with PCO would lend gravitas --- if not leverage --- to its assessment products. This combined central intelligence fusion center should be made accountable to the National Security Advisor to the Prime Minister. Its assessment products would be disseminated to clients across government, and would also be fed back to the intelligence and security agencies to help support the more proactive, calibrated strategy for countering terrorism.

The creation of a more robust and comprehensive national intelligence fusion capability would require an enhanced professionalization of Canada's intelligence analyst community. Currently, there is no professional career stream for analysts in the Canadian S&I Community, unlike in other jurisdictions. Except for D Strat A, FINTRAC and the smallish analytical units in some government departments, which do recruit analysts directly, most Canadian intelligence analysts are seconded from operational ranks for short-term assignments in analytical units. Little or no opportunity is available for career development in intelligence analysis. In order to build up its institutional capacity for intelligence analysis the Canadian S&I Community must create a professional cadre of career analysts possessing the aptitudes, skills, and commitment appropriate to this work. This implies the introduction of a professional career path for analysts, with appropriate incentives and rewards for expertise and promotions. What is called for is a transformation of the management culture of the Canadian S&I Community writ large, a cultural shift in favour of analytical tradecraft as distinct from the other dimensions of the intelligence enterprise.

The building of analytical capacity in the Canadian S&I Community and the achievement of professional standards would necessitate, in turn, the establishment of a specialist training and professional development regimen for career analysts. Currently, no such training or professional development program exists in Canada, other than a very basic entry-level module for newly assigned analysts organized under the auspices of IAS. By way of contract, the United States supports a wide spectrum of specialized training and professional development courses and programs for analysts, delivered through such institutions as the Sherman Kent School for Intelligence Analysis at the CIA University, the National Security Agency's Analysis Training Program, the FBI Academy, and the National Defence Intelligence College.

Although the Canadian S&I analytical community may be too small in size to afford a dedicated professional school of its own, at least at present, this should not inhibit the introduction of high-quality training and professional development programs for intelligence analysts through other available channels. Surely, with appropriate resourcing and political will it should be possible to design and deliver a curriculum and courses for the professional development of intelligence analysts under the aegis of existing government training institutions, such as the Canadian Police College or the Canada School of Public Service, either singly or in combination with university-based programs in Intelligence and Security Studies.

6. COORDINATING AN ALL- OF-GOVERNMENT APPROACH TO INTELLIGENCE-LED COUNTER-TERRORISM

A move towards a proactive, intelligence-led approach to counter-terrorism is predicated on the effective coordination of the national security and intelligence effort. Coordination from the centre is intended to promote seamless interaction between the producers of threat assessments, based on all-source intelligence, and the operational application of appropriate, calibrated security measures to counteract terrorist threats at each stage of the terrorism cycle. The coordinating mechanism constitutes the institutional centre-piece of a proactive, intelligence-led, proactive, calibrated all-of-government response to terrorist threats. It furthermore should serve to ensure the coherence and effectiveness of inter-departmental plans to safeguard vital national assets, mitigate consequential damage, and ensure resilience. The Netherlands Office of the National Coordinator for Counterterrorism (NCTb) represents one such central coordinating organization for some 20 Dutch agencies and departments engaged in the national counter-terrorism effort.[74]

The salience of the coordination function implies that it must be assigned to a suitably high-profile central agency of government. In Canada, probably the most appropriate locus for this enhanced coordination function would be with the office of the National Security Advisor to the Prime Minister, whose formal role at PCO includes that of coordinator

---

74 The Netherlands, Department of Justice and Department of the Interior and Kingdom Affairs, *The National Coordinator for Counterterrorism (NCTb)* (The Hague: 2005). Note that the Office of the National Coordinator for Counterterrorism is located in the Netherlands Department of the Interior and Kingdom Relations.

of the security and intelligence community. Under the proposed new arrangement, intelligence assessments from the national fusion centre at PCO would flow up to the National Security Advisor, to serve as the basis for coordinating the intelligence machinery to deal with specified threats. This proactive, intelligence-led approach implies a significant enhancement of this coordination function in order to ensure policy coherence, inter-agency cooperation, and effective synergy among a wide array of security, intelligence and law enforcement organizations, relevant government departments (at all levels), and even private owner/operators of critical national infrastructure. It is noteworthy that the recently elected Government of Australia announced its intention to proceed with the creation of a new office of National Security Advisor with authority to promote operational coordination among that country's intelligence and security community.[75]

To perform this enhanced coordination function effectively, this proposed new institutional arrangement would equip the office of National Security Advisor with three potent, instrumental resources to promote coordinated, calibrated, analysis-driven interventions:

- Supplementary budgetary appropriations
- Additional personnel allocations
- Moral suasion

Additional budgetary and personnel resources could be dispensed by the National Security Advisor to operational agencies in order to endow them with the incremental capacity needed to focus more attention on particular targets and objectives, albeit without infringing on their autonomous roles.

Of course, security and intelligence agencies, like all components of government, tend to be fully stretched, financially and staffing-wise, in performing their present tasks. Any additional assignments must call forth incremental resources, financial and personnel, to sustain operational effectiveness. The office of the National Security Advisor

---

75 Sushi Das, 'US style security chief to fight terror," *The Age* [Melbourne], 28 January 2008; see also Anthony Bergin and Mark Thomson, *An Office of National Security: Making it Happen* (Canberra: Australian Strategic Policy Institute, 2007).

would be allocated, each year, a modest number of personnel positions and budgetary funds for dispensing to the intelligence and security agencies or departments to enable coordinated operations against targets, at the instance of the National Security Advisor a intelligence and security coordinator. To be sure, each operational agency receiving supplementary resources through this route would still be accountable to Treasury Board, at the end of the financial year, for their full and proper utilization. The moral suasion emanating from the office of the National Security Advisor at the central agency of government should offer further leverage to the resource dispensations. Be that as it may, this resourcing incentive for intelligence-led counter-terrorism should make the proactive, all-of-government approach operationally viable.

The coordinating mechanism represents, in essence, the key enabler for this holistic, all-of-government approach to national security. It is the coordinating body, the office of the National Security Advisor, that would be responsible for bringing the vital elements of intelligence analysis to bear in support of proactive, calibrated interventions on the part of intelligence and security authorities to counteract the terrorism cycle. Ultimately, effective counter-terrorism requires that institutionalized excellence be built in to the architecture of the national security system.

7. AFTERWARD: BUILDING COUNTER-TERRORISM CAPACITY IN NATIONAL SECURITY CULTURE

The sustainability of any system for national security in a democracy depends, in good measure, on building and maintaining public confidence in the necessity, propriety and efficiency of the national security machinery being deployed. Public acceptance is reflected in the existence of a security culture, a broad societal recognition of the need for statutes, policy initiatives, and actual national security institutions to protect public safety against perceived threats. Security culture, in democracies, underwrites the values of human security writ large. Three core elements of a security culture will be addressed here, as being pertinent to the development of a proactive, intelligence-led architecture for counter-terrorism:

> (a) the assurance of intelligence and natural security accountability; (b) the education of citizens about national security and intelligence matters; and (c) the fostering of public awareness about the country's experience in protecting its national security.

Whereas Canada has put in place some generally respected accountability mechanisms for some components of its S&I Community, this country has been laggard, if not negligent, regarding the educational and public awareness aspects of building a national security culture. Yet, the very multicultural character of Canadian society places particular demands on a security culture especially in the current threat environment.

Many democracies, including Canada, have introduced accountability systems for their national security machinery to monitor and report on its compliance with policy, performance and statutory requirements, and thus contribute to public confidence. This accountability element of national security machinery has become all the more salient at a time when the secret services need to intervene more intrusively in domestic society to defend against threats of terrorism.[76] Up to now, public accountability for Canadian security and intelligence services has emphasized executive inspectorates and review over parliamentary oversight. This accountability system is compartmentalized by agency and also by function. CSIS is subject to scrutiny by an Inspector-General and by the independent Security Intelligence Review Committee, and CSE by a CSE Commissioner. The Auditor-General of Canada, Privacy Commissioner and Human Rights Commissioner all monitor the entire S&I Community along with other government departments and agencies in accordance with their respective functional mandates.[77] However, there is no specific accountability mechanism applicable to the RCMP national security activities, other than the more general 'complaints' process. The recommendations of the O'Connor Commission of Inquiry (Arar Commission) for establishing a more comprehensive set of mechanisms for national security accountability that would also encompass the RCMP in its national security role, along with other pertinent security agencies like CBSA and FINTRAC, and departments like Citizenship and Immigration Canada and the Department of Foreign Affairs and International Trade, still await a government decision on implementation.[78]

---

76 Paul Wilkinson, *Terrorism and Liberal Democracy*. (London: Macmillan, 1999); Rudner, "Challenge and Response," pp. 31-34.

77 Gary Filmon, "The Canadian Model of Security and Intelligence Review," in *Accountability of Intelligence and Security Agencies and Human Rights* (The Hague: Review Committee on the Intelligence and Security Services (CTIVD) & Faculty of Law, Radboud Universiy Nijmegen, 2007); Martin Rudner, "Contemporary Threats, Future Tasks: Canadian Intelligence and the Challenges of Global Security," in Norman Hillmer and Maureen Appel Molot, eds., *Canada Among Nations 2002. A Fading Power* (Toronto: Oxford University Press, 2002).

78 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National* Security *Activities* (Ottawa: Public Works and Government Services Canada, 2006).

Parliamentary oversight of the S&I Community is relatively weak in Canada as compared to the more cogent role played by American, British or Australian counterparts. Indeed, Canadian governments and intelligence services have tended to minimize their exposure to parliamentary scrutiny. Consequently, the Canadian Parliament has not emerged as a forum for deliberations on intelligence policy, finance, or operational accountability. The committee structure of the Canadian Parliament has, paradoxically, militated against effective oversight of the S&I Community. While the Senate Standing Committee on National Security and Defence has conducted hearings on wide array of national security issues, the House of Commons' committee structure is organized around specific departmental portfolios, thereby dispersing deliberations on Security and Intelligence matters amongst a host of separate committees and sub-committees. There has been some discussion in recent years about creating a proper Parliamentary Committee on Intelligence and National Security, however it remains to be determined whether this will come to pass. For the Parliament to become an effective player in upholding national security accountability, it is clear that Canadian legislators will need to demonstrate the same breadth of purview, continuity of committee membership, and access to intelligence sources that exemplify their American or British counterparts.

An educated public represents a vital asset for creating and sustaining a vibrant security culture. Despite the heightened public attention directed at National Security and Intelligence matters especially since September 11th, the capacity of Canadian institutions of higher education to exercise knowledge leadership in these fields remains grossly inadequate. Canadian students have demonstrated an extraordinarily strong interest, in their numbers and in aptitude, in pursuing undergraduate and post-graduate studies on Intelligence and National security subjects.[79] Yet, Canadian universities have been painstakingly slow to respond to societal demand. Very few university courses or programs dealing with Intelligence and/or National Security studies are currently on offer in Canada. Carleton University stands out as host to Canada's only graduate program in Intelligence and National Security under the aegis of the Norman Paterson School of International Affairs, while also offering dedicated

---

79 Mark Cardwell, "Intelligence Failure," *University Affairs* [Association of Universities and Colleges of Canada], February, 2008, pp. 25-27.

undergraduate courses in History and Political Science. It remains to be seen whether the new graduate schools of international studies recently announced at the universities of Ottawa and Waterloo/Wilfrid Laurier will choose to include Intelligence and Security in their repertoires. One especially shameful facet of the present educational lacunae is the paucity of learning material on Canada's own intelligence history. Other than singular books and a few scholarly articles in international journals, Canada's distinguished intelligence history remains virtually unknown to students and people in this country.

We should note, parenthetically, that the prospective expansion of Canada's intelligence analysis/assessment capabilities would require recruits with specialized academic qualifications. It would be incumbent on Canada's universities, and their programs in Intelligence and Security Studies, to help generate the high-level expertise likely to be needed. Among the disciplines likely to be most in demand are international area studies and languages, conflict analysis, mathematics, finance, sociology and anthropology, psychology, law, computer science, and engineering, as related to intelligence, security, and terrorism.

Existing deficiencies in Canada's higher education system also reflect themselves in a weak national capacity for academic research into vital issues of national security interest, including terrorism. In 2002 Carleton University established the Canadian Centre of Intelligence and Security Studies, Canada's first -- and so far only -- dedicated research centre focusing on Security and Intelligence topics. While valuable work has been done, by all accounts, research remains grievously constrained by a dire lack of financial support, even from the official funding councils, coupled with acute staff shortages. It is indicative of the absence of priority that out of more than 1,800 Canada Research Chairs established in Canadian universities since 2000 under that federal initiative to promote academic excellence in priority fields identified by the universities themselves, not a single one was dedicated to Intelligence Studies. Not one. Just one Canada Research Chair relating to terrorism studies was recently established at Université Laval in Quebec City. Compared to the rather more dynamic situation in American, Australian and British universities and research institutions, Canada's educational and research capacity in these fields of vital national security concern remains woefully under-strength.

Despite their few numbers, and notwithstanding their being scattered among a dozen or so universities across the country, the small coterie of Canadian academic specialists has made a signal contribution to building up one of the world's foremost organizations in the field, the Canadian Association of Security and Intelligence Studies (CASIS). This association is run jointly by Canadian academics and practitioners. It convenes annual conferences, alternating between venues in Ottawa and in elsewhere across Canada. These conferences attract a large attendance from academics, government officials, journalists, private sector representatives, students, and others, from Canada and abroad. Issues addressed at these CASIS conferences are highly topical, presented by renown authorities, and are often well covered by the media. Still, for all of its success in bringing knowledge about Intelligence and Security matters to Canada and to Canadians, CASIS continues to subsist with barely minimal administrative and financial support. Public awareness and knowledge building about Intelligence and National Security are still not priorities, neither for Canadian governments nor for private foundations, so that even a globally acclaimed CASIS is left to endure hand-to-mouth, year to year.

Fostering public awareness about national security matters is vital for the sustainability of a security culture in a democracy. Ordinarily, public awareness in most spheres of governance, like the economy or social policy, rests on some degree of policy transparency. Understandably, transparency is inherently problematic with respect to security intelligence activities, and especially with regard to operational matters that must remain secret. Other means must therefore be used to acquaint the citizenry with Security and Intelligence issues in order to build trust. Media relations certainly have an important role to lay in purveying reliable information to journalists and through them to the public. A high standard of media reportage and comment can contribute invaluably to promoting greater public familiarity with, and knowledge of, Intelligence and National Security affairs. Likewise, the opening and declassification of historical intelligence archives can contribute invaluably to the extension of public knowledge about this country's experience in Intelligence.[80] It would also reinforce the point that Intelligence has long been a legitimate arm of Canadian statecraft. Ironically, Canada's intelligence archives

---

80 Wesley Wark, "The Access to Information Act and the Security and Intelligence Community in Canada." Research Study #20, Report of the Access to Information Review Task Force, *Access to Information: Making it Work for Canadians* (Ottawa, 2002).

dating back to the Second World War remain classified and therefore closed. Opening access to that material would surely help encourage the writing of histories that augment the knowledge resources available to educators and to society at large.

Museums can also play a valuable part in enhancing public familiarity and understanding of complex and remote phenomena. Certainly, the Secret War gallery at the Imperial War Museum in London, and the privately supported International Spy Museum in Washington, D.C. have helped inspire a greater public awareness and appreciation of the role of intelligence and security services in responding to contemporary threats to the national security. These exhibits have been immensely popular, by all accounts. There is no museum in Canada that exhibits the artifacts of our own Intelligence and Security experience, conveying our distinguished record to a mass public. If there is ignorance abroad among Canadians, the cause may be a failure to consider the importance of investing resourcefully to publicize our Intelligence and Security legacy through institutions of mass culture.

Security culture can be an enabler of sustainable intelligence reform. Just as security and intelligence machinery in democracies needs to be lubricated with an appropriate level of public confidence, so transforming the S&I architecture calls for an even greater degree of public awareness and understanding of the parameters of change. Fostering a broad based security culture grounded on public confidence in the accountability mechanisms, on knowledge of national security matters, and on civic trust in the appropriateness of security and intelligence measures, would make Canadians all the more amenable to, and supportive of new initiatives aimed at dealing with sensitive issues like counter-terrorism. It behooves government to be mindful of the importance of security culture as a key enabler of sustainable capacity building in addressing the prospective transformation and revitalization of Canada's Security and Intelligence Community.

Martin Rudner is a Distinguished Research Professor Emeritus at The Norman Paterson School of International Affairs, Carleton University, Ottawa, and was founding Director of the Canadian Centre of Intelligence and Security Studies at Carleton. Professor Rudner was born in Montreal, Quebec, and was educated at McGill University, the University of Oxford, and Hebrew University of Jerusalem, where he received his doctorate. He is author of over ninety books and scholarly articles dealing with international affairs, Southeast Asia, and Intelligence and Security studies. Recent publications include: "Protecting North America's Energy Infrastructure Against Terrorism," *International Journal of Intelligence and CounterIntelligence* (2006); "Canada's Communications Security Establishment, Signals Intelligence and Counter-terrorism," *Intelligence and National Security* (2007); and "Misuse of Passports: Identity Fraud, The Propensity to Travel, and International Terrorism," *Studies in Conflict and Terrorism* (2008). Professor Rudner has consulted and lectured on security and counter-terrorism issues to various departments and agencies of government, and has given expert testimony before courts, commissions of inquiry, and parliamentary committees. He served on the Advisory Panel for the Policy Review component of the Arar Commission of Inquiry under Mr Justice Dennis O'Connor.

The Intelligence-Law Enforcement Nexus:

A study of cooperation between the Canadian Security Intelligence Service and the Royal Canadian Mounted Police, 1984-2006, in the Context of the Air India terrorist attack

Professor Wesley Wark
Munk Centre for International Studies
The University of Toronto

Preface

The destruction of Air India flight 182 by a terrorist bomb remains one of the most important, but understudied, events in modern Canadian history. The published literature on the Air India disaster is scanty and dominated by journalistic accounts. Archival documents remain, for the most part, inaccessible due to security classifications and the absence of any systematic release policy for historically significant federal government records (apart from Cabinet documents). The main body of evidence in the public domain is a product of government mandated studies, the work of the Security Intelligence Review Committee (SIRC) and trial records surrounding efforts to prosecute the alleged perpetrators of the bombing.

Given these circumstances, any study of any aspect of the Air India tragedy conducted on the basis of public documents alone will face significant limitations. The main concern is the inevitable reliance on judgments arrived at in the government studies and by SIRC, without the opportunity to thoroughly assess the evidence on which such judgments were based.

The nature and evolution of cooperation between the Canadian Security Intelligence Service and the Royal Canadian Mounted Police is at the heart of the story of how the Canadian government responded to the threat of Sikh terrorism and how it reacted in the aftermath of the Air India bombing. Despite the limitations of publicly available material, it is possible to arrive at some potentially important conclusions about the state of CSIS-RCMP relations between the birth of CSIS in 1984, one year prior to the Air India bombing, and the issuance of a revised agreement between CSIS and the RCMP in September 2006, meant to put a new face on the relationship between our security intelligence and security enforcement agencies.

An effective counter-terrorism policy contains many ingredients. One of these is good cooperation between intelligence and police forces. In studying the evolution of CSIS-RCMP cooperation in the context of the Air India affair we are looking to assess the quality of the relationship over a period of years, the stress points, and any problems inherited from the past that remain to be fixed.

The Rae Report

In the aftermath of the March 2005 acquittal of two defendants in the Air India bombing, and amidst on-going public controversy, the Government of Canada asked The Honourable Bob Rae to provide "independent advice on what remains to be learned about this tragedy." The Rae report, "Lessons to be Learned," was produced in late November 2005.[1] Mr. Rae zeroed in on four issues that he believed demanded further study. Three of the four areas of concern involved questions of intelligence work and cooperation between the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP). Mr. Rae believed it was important to establish whether the intelligence assessment process worked adequately and whether any systemic issues emerged that have not been resolved. His review, moreover, had led him to believe that "problems" existed in the relationship between CSIS and the RCMP that may have affected intelligence gathering and criminal investigations. Mr. Rae also felt that the history of the Air India tragedy illustrated the difficulties that exist in trying to establish a link between security intelligence and evidence that can be used in criminal proceedings.[2] He advocated the establishment of a further policy-oriented public inquiry into the lessons of Air India that would take up the issues he identified and provide answers to them relevant to Canada's current efforts to combat terrorism.[3]

Mr. Rae's recommendation was speedily accepted and he was appointed to head such a public inquiry in November 2005. That inquiry was abandoned by the newly elected Conservative government in 2006, which delivered on its own promise to hold a full judicial inquiry into the Air India bombing. On May 1, 2006, the Honourable John C. Major was appointed as Commissioner to conduct an inquiry into the bombing of Air India Flight 182. His appointment directed that he give consideration to the findings of previous studies of the issue, including the Rae report. The terms of reference for Justice Major's inquiry drew on the Rae report by identifying deficiencies in threat assessments, problems in effective cooperation between CSIS and the RCMP and the challenges of establishing linkages between security intelligence and evidence in criminal trials as among the key issues to be studied.[4]

---

1 The Honourable Bob Rae, "Lessons to be Learned," November, 2005. Available online at www.publicsafety.gc.ca
2 ibid., p. 22
3 ibid., p. 31
4 Order in Council, Privy Council, 2006-293, May 1, 2006

In both the Rae report and the terms of reference for Justice Major's Inquiry issues of intelligence threat assessments, CSIS-RCMP cooperation, and the continuum between intelligence and evidence are all treated as separate and distinct issues. In this research report I will endeavour to probe the linkages and synergies between these issues in the broad context of the evolution of CSIS-RCMP relations. Questions about the quality and use of threat assessments, about the nature of relations between our civilian security intelligence agency and our federal law enforcement agency, and regarding the transmission of intelligence information into evidence are, in my view, inseparable and are rooted in the history of our intelligence structures and policies.

Historical Background

The Canadian Security Intelligence Service was established by law in 1984. Its creation was a product of the recommendations issued by the McDonald Royal Commission, which studied the activities of the RCMP Security Service and found evidence of both illegalities in its conduct of operations, especially with regard to the monitoring and disruption of separatist groups in Quebec, and a general failure of performance when confronted with a complex range of national security threats. In removing the security intelligence function from the Royal Canadian Mounted Police, where it had resided since 1920 and, in predecessor organizations as far back as 1864, the government of the day opted for a distinct separation of powers and mandates. The creation of CSIS was meant to establish a civilian intelligence service better equipped to understand threats to national security. CSIS would be embedded in law (the CSIS Act) and its operations reviewed by both internal and independent bodies—the Inspector General and the Security Intelligence Review Committee respectively. At the same time, it was understood that the RCMP would continue to play a role in investigations of national security offences.

While there is evidence to suggest that problems in relations between the newly created CSIS and an RCMP shorn of its security intelligence function were anticipated, it is fair to say that the major concern in the early years of CSIS was with establishing its civilian character and getting it up and running. These early years, of course, overlapped with the tragic events of the Air India bombing, which occurred only a year after the birth of CSIS.

The security intelligence system that was established with the creation of CSIS was a radical departure for Canada from past practice. It aligned the Canadian approach more closely to that of Britain and other Commonwealth countries, where a separation of mandates between security intelligence and law enforcement was reflected in separate agencies. At the same time, the new system distanced Canada from the institutional set up of its American ally, where the Federal Bureau of Investigation contained both a law enforcement and security intelligence function. By the mid-1980s, Canadian intelligence alliance connections had shifted their centre of gravity from a long embrace of British practice and partnership, dating back to World War Two, to a close relationship with the United States intelligence community. Opportunities for learning lessons at the outset about how to make the new system work were, accordingly, reduced. Moreover, the idea of constructing a security intelligence system on the basis of individual departments and agencies each pursuing specialized and distinct mandates with little centralisation or control suited the historical pattern of Canadian intelligence practice dating back to World War Two. A Cold War nomenclature came to stick as a descriptor of the Canadian system—it was based on "silos"--self-contained and autonomous units of secret activity with little connection between them.

Sikh terrorists struck against Air India flight 182 in June 1985 while CSIS was still in its infancy. When the Air India plane was blown out of the skies, the Canadian government suffered a grievous intelligence failure. But these historical propositions—infancy and intelligence failure—need to be kept separate in order to resist the temptation of assuming that infancy explains intelligence failure, and by extension that infancy overcome negates the need for any on-going scrutiny of the causes of intelligence failure.

The failure of intelligence is a critical dimension of the Air India story. Intelligence failure was a product of the inability of Canada's newly created intelligence and counter-terrorism service, CSIS, and its long-established federal police counterpart, the RCMP, to fully target and successfully assess the threat posed by Sikh terrorism. Without a clear intelligence picture, CSIS and the RCMP could neither prevent nor pre-empt the attack. Deficiencies in intelligence hampered the prosecution of the perpetrators involved, especially in the crucial early stages . Studying the intelligence failure at the heart of Air India forces us to ask questions about the capacity of intelligence and police agencies to cooperate successfully

and work together towards a common counter-terrorism objective. Air India also compels us to ask how well and wisely lessons were learned, specifically about the nature of intelligence and RCMP-CSIS cooperation, in the years subsequent to the events of 1985.

An effort to answer these questions will not prevent future terrorist attacks in Canada or against Canadian interests overseas. But it might serve to increase Canadian capacities and understanding in the face of future threats, help fashion realistic policies and, from a public perspective, establish realistic expectations of government performance.

The Lineaments of Intelligence Failure

The causes of intelligence failure have attracted considerable scholarly attention in the literature of intelligence studies. Employing case study techniques and detailed analysis of available documentation, on episodes ranging from the Battle of Jutland in May 1916, to Operation Barbarossa and Pearl Harbor in 1941, the Cuban Missile Crisis in 1962, the Yom Kippur War in 1973 and, in a contemporary vein, threat assessments on Iraq's supposed weapons of mass destruction program in 2002-03, scholars have come up with a rich tapestry of ideas on the root causes of intelligence failure.[5] Much of this analysis has been guided by an understanding of how the intelligence process works. In this regard the concept of the "intelligence cycle" has been of heuristic value. The intelligence cycle dissects the critical activities of an intelligence system, identifying these as tasking, collection, analysis and dissemination.[6]

Intelligence failures are a product of the systemic breakdown of one or more of these critical activities. Each part of the process is complex, demanding and fragile. Their totality, which is meant to prioritize tasks for

---

5 On intelligence and the Battle of Jutland in 1916, see Patrick Beesly, Room 40: British Naval Intelligence 19145-1918 (New York: Harcourt, Brace, Jovanovich, 1982, ch. 10. The most recent analysis of Operation Barbarossa is David Murphy, What Stalin Knew (Yale University Press, 2006). On Pearl Harbor, the classic account by Roberta Wohlstetter, Pearl Harbor: Warning and Decision (Stanford University Press, 1962) remains outstanding. The Cuban Missile Crisis is examined in James G. Blight and David Welch, eds., Intelligence and the Cuban Missile Crisis (London: Frank Cass, 1998). Israeli intelligence failure in the run-up to the Yom Kippur war has been analysed incisively by Avi Shlaim, "Failures in National Intelligence Estimates: The Case of the Yom Kippur War," World Politics, 28, no. 3 (April 1976), 348-80. Studies of the failure of intelligence with regard to Iraq WMD are now legion, but one of the best accounts is Lawrence Freedman, "War in Iraq: Selling the Threat," Survival, 46, no. 2 (Summer 2004), 7-50.

6 See the definition employed by the Central Intelligence Agency, "The Intelligence Cycle," at www.cia.gov/cia/publications/facttell/intelligence_cycle.html

intelligence services and generate accurate information that is suitably and promptly communicated to decision-makers, is subject to a high risk of failure. In historical case studies of intelligence failure, a cascading effect is often present. Poor tasking will contribute to inadequate collection, which will in turn rob assessment of sufficient capacity to develop sophisticated judgments. A hollowed out intelligence process will generally fail to create the dissemination (and feedback) channels so vital to establishing the usefulness of intelligence and aiding policy-making.

Intelligence failures inevitably contribute to flawed policy and inadequate operational responses. But an important distinction between intelligence, policy and operations needs to be maintained, while accepting the blurred boundaries between them. Intelligence failures reveal pathologies of knowledge and learning, They are all about the sources of misperception. Policy failures and operations outcomes may be rooted in intelligence misjudgement and error but are not uniquely determined by them.

Unhappily, intelligence failures may be ubiquitous. One of the seminal discussions of intelligence finds that, "Intelligence failures are not only inevitable, they are natural." Richard Betts builds to this fatalistic conclusion by way of careful reasoning about the inevitable presence of pathologies of judgement, ambiguity and ambivalence surrounding information flows, the imperfections of bureaucratic structures, and the phenomenon of political decision-makers driven to consider themselves their own best intelligence analysts. Betts ends by stating: "My survey of the intractability of the inadequacy of intelligence, and its inseparability from mistakes in decision, suggests one final conclusion that is perhaps most outrageously fatalistic of all: tolerance for disaster."[7]

The main difficulty with this argument, apart from its unpalatable nature, is that tolerance for disaster can blunt efforts to improve systems and performance and learn lessons from the past. What does emerge usefully from the work of Richard Betts and a host of other writers on intelligence failure is an appreciation of the complexities of intelligence work and the sources of failure: an appreciation that focuses on analytical misjudgment as a central and perennial factor.

---

7 Richard Betts, "Analysis, War and Decision: Why Intelligence Failures are Inevitable," World Politics, 31, no.1 (October 1978), 89

There is nothing determinative about this finding, but the literature on intelligence failure can serve as a guide to investigations into the intelligence dimension of Air India. It provides us with a investigative road map, with tasking, collection, assessment and dissemination all marked out as potential zones of error. It also suggests that we pay close attention to intelligence assessment –both the product and the institutional setting--as the key to intelligence performance.

The Seaborn Report

The very first post-mortem conducted by the Canadian government into the events of Air India was directed by the newly established office of the Security and Intelligence Coordinator, a post held by Blair Seaborn. Mr. Seaborn had a long and distinguished career with the Department of External Affairs before assuming the post of Coordinator, a career which included substantial exposure to intelligence activities, particularly while serving overseas. Yet the "Seaborn" Report," in actual fact a product of the coordinating mechanism of the Interdepartmental Committee on Security and Intelligence, downplayed the significance of the role of intelligence with regard to both Air India and future terrorist attacks.

The Seaborn report, issued on September 24, 1985, noted that the Canadian authorities were alert to the general possibility that Air India could be a target of Sikh terrorism but lacked any specific intelligence on this threat.[8] In a brief discussion, the report found no fault with the intelligence system, but also cast doubt on its wider utility. It argued that intelligence on specific terrorist targets was "rarely forthcoming," and that efforts to improve intelligence collection were likely to have only marginal use.[9] According to the Seaborn report, intelligence could not be relied on "as the principal, let alone the sole, means of countering terrorism."[10] Instead the task of intelligence was to assist in determining appropriate levels of security, a function deemed "important," that would rely on good assessment and dissemination.

---

8 Interdepartmental Committee on Security and Intelligence, "Report on Security Arrangements Affecting Airports and Airlines in Canada," September 24,1985, p. 1. Hereafter cited as "Seaborn Report." Available online at www.psepc.gc.ca/prg/ns/airs/ai_rep-en.asp

9 ibid., p. 2

10 ibid

Effective counter-terrorism was not to rely on intelligence, but rather on "a regime of sufficiently rigorous security in respect of likely targets to deter a terrorist or similar incident from achieving success."[11] The remainder, and bulk, of the report dealt with airport and airline security issues.

There are echoes, probably unconscious ones, in this initial post mortem of some of the analysis arrived at years earlier by Richard Betts. Expectations of intelligence performance must be grounded in reality, failures anticipated, attention paid to analytical and dissemination processes.

But the minimalist position on intelligence taken in the Seaborn report also reflected contemporary government attitudes towards the intelligence function. The absence of any substantial expectations about intelligence performance blunted any serious critique of intelligence shortcomings or any close look at the effectiveness of CSIS-RCMP cooperation. The Seaborn report was compiled at a time when the post bombing investigation was still in its early phases and no "hard" information was available on the perpetrators, or even the exact nature of the destruction of Air India Flight 182. Moreover the report was the product of a committee and of a system that depended on input from the key intelligence agencies, including the RCMP and the Canadian Security Intelligence Service. The power and authority of the Security and Intelligence Coordinator were untested. All of these factors may have constrained a fuller understanding of the role of intelligence and limited any impulse towards sustained and probing criticism. However, the actual dynamics behind the work of ICSI and the compilation of the Seaborn report cannot be ascertained on the basis of public documentation, as the relevant records, assuming they exist, are not in the public domain.

The first two recommendations of the Seaborn report faithfully convey a sense of the limited intelligence function. They urged that the key government agencies, Transport Canada, CSIS and the RCMP should have the requisite assessment capacity and that threat assessments and dissemination channels should be regularly reviewed by an interdepartmental committee led by the Department of the Solicitor General.[12] It is not known from the public record whether even these

---

11 ibid
12 ibid., Annex B, p. 9

modest proposals for adjustments to capabilities and bureaucratic operations were followed through.

SIRC: The Early Reports

The CSIS Act had established an independent review mechanism for the new agency, in the form of the Security Intelligence Review Committee. SIRC prepared an annual report card for the Minister and Parliament on CSIS's fidelity to its mandate, the law and Ministerial direction. Early SIRC reports, beginning in 1985, called some attention to CSIS-RCMP cooperation, on occasion using the phrase "healthy tension" to describe the state of affairs. The most pointed concern expressed by SIRC in the early years emerged in the third annual report, produced in the Fall of 1987, in which it noted the need for scrutiny of the existing CSIS-RCMP Memorandum of Understanding, and greater Ministerial involvement.[13] As far as SIRC was concerned, the roles of CSIS and the RCMP were complementary. The greatest friction was likely to occur in regard to counter-terrorist cases, where the RCMP's mandate to conduct national security investigations and CSIS's mandate to collect security intelligence might well overlap. SIRC wanted, at best, some fine-tuning of the system to make sure that cooperation flourished in practice as it should in theory.

In general, SIRC's concern in the early years of observing CSIS was to ensure that the new agency met the objectives laid down by the McDonald Commission and the subsequent CSIS Act, especially to ensure that it growing into an effective civilian intelligence service. Theoretical and practical issues of how the new agency would interact with the RCMP in its national security mandate were peripheral to this central concern.

The Osbaldeston Report

In another indication that CSIS-RCMP cooperation was not seen to be a core issue at the time, the report of an Independent Advisory Team, established by the Solicitor General following concerns about CSIS' early performance, focused attention on critical deficits in leadership, human resource management and training, targeting, and intelligence

---

13 Security Intelligence Review Committee, Annual Report, 1986-1987, p. 29. Available online at www.sirc-csars.gc.ca

production. Questions concerning the nature of the CSIS-RCMP relationship did not emerge in the study chaired by Gordon Osbaldeston, completed in October 1987.[14]

Parliamentary Review of the CSIS Act

Similarly, the mandated Parliamentary review of the CSIS Act, conducted in 1989-1990, gave only passing attention to questions of CSIS-RCMP cooperation. It noted some concerns with cooperation below the headquarters level, but also pronounced itself satisfied with the general spirit and intent of the existing CSIS-RCMP Memorandum of Understanding (MOU), revised in 1989.[15] The Committee's report did flag a concern about the "serious technical problems to be overcome regarding the process by which intelligence generated by CSIS can be transformed into criminal evidence," but also commended the establishment of a "technical" committee in the Department of Justice to study these problems on an on-going basis.[16] Not a single one of the Committee's 117 recommendations referred specifically to CSIS-RCMP relations.

In the early years of CSIS's existence, which overlap with the Air India bombing and the first phase of investigative activity into the attack, the cumulative record of study by a variety of review bodies suggests that relatively little attention was paid to either the question of intelligence failure or the specific dynamics of CSIS-RCMP relations.

SIRC'S 1992 Study of AIR INDIA

There would, in fact, be a seven year wait following the Seaborn Report until any further systematic, external study of the intelligence underpinnings of the Air India attacks was undertaken. SIRC had maintained a watching brief on Air India while the RCMP investigation proceeded, but in November 1992 completed a massive study entitled "CSIS Activities in Regard to the Destruction of Air India Flight 182."[17] .

---

14 Solicitor General Canada, "People and Process in Transition: Report to the Solicitor General by the Independent Advisory Team on the Canadian Security Intelligence Service, October 1987

15 House of Commons, Report of the Special Committee on the Review of the CSIS Act and the Security Offences Act, "In Flux But not in Crisis," September 1990, p. 105.

16 Ibid.

17 Security Intelligence Review Committee, "CSIS Activities in Regard to the Destruction of Air India Flight 182 on June 23, 1985," November 16, 1992. Originally classified Top Secret. ATIP version courtesy of the ATIP office, SIRC

The SIRC report had the advantage over Seaborn of time, a clearer understanding of the likely causes of the Air India attack, dedicated independent resources, and a determination, stemming from the review body's mandate, to put CSIS performance under a spotlight.

The SIRC study discovered that the problem of Sikh extremism had been scrutinized by CSIS's predecessor, the RCMP Security Service, beginning in late 1974. [18] Some concern was maintained following the establishment of three so-called "Khalistan Consulates" in Canada to promote the idea of an independent Sikh homeland.[19] But the event that prompted significant attention to the threat of Sikh extremism in Canada, was the reaction of Sikh Canadians to the Indian government's assault on the Sikh Golden Temple at Amritsar in June 1984.[20] All of this was brewing as the Canadian Security Intelligence Service was launched on July 16, 1984. Sikh extremism in Canada became one of the first targets of the newly minted CSIS. One of the earliest channels of CSIS reporting on threats to the RCMP was opened by assessments provided to the RCMP VIP Security branch in this period.[21]

Further early forms of CSIS-RCMP cooperation on Sikh extremism emerged as the one year anniversary of the Amristar massacre approached in June 1985. On May 6, 1985, an interdepartmental working group was established consisting of members of the RCMP, CSIS, External Affairs (now DFAIT) and the Ministry of the Solicitor General.[22] The mandate of this working group was to consider risks associated with the anniversary and the level of protection afforded to Indian diplomatic personnel and establishments in Canada.[23]

CSIS-RCMP cooperation in the weeks immediately preceding the Air India bombing had a regional dimension as well. Both agencies engaged in decentralized operations, with regional offices playing a major role in intelligence collection for CSIS and criminal investigation for the RCMP. A CSIS surveillance team from the BC region had Talwinder Singh Parmar, a prominent self-styled Sikh preacher and proponent of an independent Khalistan, in their sights and shared some of their findings with E division

---

18 ibid., p. 4
19 ibid
20 ibid., p. 8
21 ibid., p. 10, 12
22 The Rae Report places the date as May 17, 1985 (p. 6)
23 ibid., p. 18

of the RCMP, based in Vancouver, which had its own VIP security and NCIS (National Criminal Intelligence Service) offices. Among the information shared was the surveillance of a Parmar trip to Nanaimo which involved a journey into the woods by Parmar and Inderjit Singh Reyat and the subsequent detection of a "loud report," thought at the time to be a rifle shot, but later discovered to be the testing of an explosive device.[24] Reyat was eventually to be convicted of manslaughter for his role in the Air India bombing. Parmar, killed in an encounter with Indian police in 1992, was to be characterized as the main perpetrator of the attack.

The SIRC analysis of the archival records makes clear that both CSIS and the RCMP were engaged by the threat posed by Sikh extremism, that CSIS information was flowing to the RCMP, and that the RCMP had sufficient appetite for such reporting to ask independently for updated threat assessments. Altogether some 70 threat assessments concerning Sikh extremism and aviation security were disseminated by CSIS to other government agencies in the period from the founding of CSIS on July 14, 1984 to June 1, 1985. Most of these assessments went to the RCMP VIP Security branch.[25] SIRC concluded both that CSIS had no specific information in advance of the threat to Air India flight 182 and that no significant gap existed prior to the bombing in CSIS-RCMP exchanges of information.[26]

It is equally clear from the SIRC study that CSIS's capacity to fully exploit technical surveillance of Talwinder Singh Parmar was lacking (primarily due to lack of linguistic talent) and that the resources devoted to sustaining full-time physical surveillance of Mr. Parmar in the critical period prior to the Air India bombing were inadequate. There are, in the lineaments of the Air India bombing, clear indications of a failure of intelligence collection.

Questions surrounding failures or weaknesses of assessment are more speculative, but it seems evident that early CSIS threat assessments lacked specificity, and suffered from a set of uncritical presumptions about the nature and targets of any Sikh terrorism. It was presumed that the most likely target for any violent reaction to mark the anniversary of Amristar

---

24 ibid., p. 22
25 ibid., p. 27
26 ibid., p. 28

would be the Indian Prime Minister's son, Rajiv Gandhi, during his visit to the United States in early June. Such a reading was fed by the concerns of US security agencies, above all the FBI, who were themselves seized by this fear and in touch through liaison channels with the Canadian authorities.

When it came to the issue of aviation security, the traditional concern about hijacking was uppermost in the minds of Canadian security officials and may have blunted more imaginative consideration of alternative threat scenarios, such as an effort to bomb a plane in flight. Such warnings as circulated about threats to civil aviation seem to have been affected by a "cry-wolf" syndrome. A series of alerts, many originating from the Indian government, all without apparent foundation, ultimately may have resulted in a kind of fatigue about such threats.

SIRC found no indication of serious problems of cooperation between CSIS and the RCMP prior to the disaster and was emphatic in its conclusion on that point. [27] With Air India, we are in the presence of an intelligence failure marked by the usual cascading effect of inadequate collection and weak assessment, but we are not, at least according to SIRC, in the presence of any systemic breakdown of inter-agency relations on the dissemination front.

The real issue of CSIS-RMCP cooperation emerges over concerns about the handling of the investigative phase of operations following the bombing itself. A memorandum of understanding had been signed between the nascent CSIS and the RCMP on July 17, 1984, to govern the transfer and sharing of information.[28] This first CSIS-RCMP MOU was based on the express need for full and mutual sharing of intelligence on national security threats and offenses, real or potential. It delineated the respective mandates of the two agencies and also identified the need for care and control over the dissemination of intelligence and the right to protect sources of information. If there was any tension in the document, it was an inherent tension involving the desire to share information while respecting distinct mandates and distinct sensitivities over sources.

The CSIS-RCMP MOU was backed up by a Ministerial directive to CSIS penned by the Solicitor General, Bob Kaplan, on July 29, 1984, and copied

---

27 ibid., pp. 35, 36.
28 The 1984 MOU is reproduced as Annex A in the SIRC study of 1992.

to the Commissioner of the RCMP.[29] As SIRC comments, the Ministerial directive "made it clear that the separation of the security intelligence role from the RCMP must not inhibit the passage of information between the RCMP and CSIS."[30] The problem was that the theory of information sharing in the aftermath of a national security incident had never been tested in practice, nor had CSIS and the RCMP enjoyed much time to allow their separate identities in the national security field to mature.

Closing the gap between theory and practice should have been a responsibility of the senior management of CSIS at the time. SIRC was critical of a failure on the part of the CSIS director and his deputy directors to communicate any clear guidance to the organization on how to "plug in" with the police investigation immediately after the destruction of Air India Flight 182.[31] Instead, ad hoc responses from the regional offices of CSIS filled the gap, with the CSIS BC region playing the most important role. [32] From the regional offices situation reports and accounts of cooperation with the RCMP flowed into headquarters. SIRC concluded that operational level cooperation between CSIS and the RCMP "appeared to be good" in the immediate aftermath of the Air India attack.[33] At the senior official level, one disquieting item of correspondence between CSIS and the RCMP was captured and noted by SIRC, but the available evidence suggested that it had no long-term effect on the working relationship between the two agencies.

The critical issue of how information derived from CSIS sources might be used by the RCMP was brought to the fore by RCMP efforts to draw on CSIS material in affidavits in support of warrants for communications intercepts on key suspects, including Parmar and Reyat. The RCMP's desire to advance its investigation came into conflict with CSIS' concern to protect its sources and methods. CSIS's initial view was that its material should be used by the RCMP to provide "investigative leads" only and should not be brought into the legal domain in applications for warrants. SIRC notes that "lengthy negotiations" took place over this issue in late 1985 (October and November), but that they resulted in an agreement on use of CSIS information by the RCMP as well as RCMP access to CSIS

---

29 The Ministerial Directive, "Bill C-9 and the Conduct of RCMP Security Responsibilities," is included as Annex B of the SIRC 1992 study.
30 Ibid., p. 38
31 ibid., pp. 41, 56
32 ibid., p. 42
33 ibid., p. 44

files for "analysis" purposes. This agreement was reached in November or December 1985.[34] The specifics of the resolution of this issue were conveyed in a briefing given by the RCMP Commissioner to SIRC on February 11, 1992. The Commissioner noted that "CSIS provided the Force with authority to use their information in pursuit of search warrants with the understanding that the information would be paraphrased in a certain manner so as to protect the identity of CSIS sources and methods of operations."[35]

A final chapter in the SIRC 1992 study involved the controversial issue of the erasure of intercept tapes generated by CSIS in the course of their surveillance of Talwinder Singh Parmar between March and July 1985. It is fair to say that SIRC found surveillance tape policy in disarray in 1985. That disarray was a product of an effort to both distance CSIS from the evidentiary role of the former RCMP Security Service while at the same time carrying on communications intercept policy in modified form from RCMP days. Disarray in policy was matched by wholly inadequate resources to process the intelligence take from the Parmar electronic surveillance, as the CSIS BC region had no suitable translator to handle Punjabi. Two days before the Air India bombing, approximately 100 audio surveillance tapes remained untranslated.[36]

In the aftermath of the Air India bombing, only 54 of a total of 210 Parmar audio surveillance tapes survived erasure, undertaken according to contemporary CSIS policy, such as it was. Those that survived did so, in effect, accidentally. Fifty tapes were retained because while they had been reviewed by an RCMP investigator they were not deemed to have been studied by CSIS independently for their intelligence value. Four tapes were retained for technical voice print analysis.

The question of information lost through erasure remains open, though in theory, and according to CSIS statements, all the erased tapes were first processed, which means they were listened to, translated and transcribed. SIRC believes it "unlikely that any information in the erased tapes indicating plans to bomb the aircraft would have escaped the attention of the monitors, translators and investigators." SIRC goes on to say that: "The RCMP determined from the translator/transcriber logs of the erased

---

34 ibid., pp. 55 and 63. Note that testimony from Reid Morden, CSIS Director, and the RCMP Commissioner differ on the date.

35 Ibid., p. 63

36 ibid., p. 75

tapes and from the 54 tapes retained and reviewed by them after the disaster, that no significant criminal information was revealed."[37]

Nevertheless, CSIS policy on surveillance tapes at the time was inadequate to serve both the agency's needs and those of the RCMP. It took four years to modify the policy, but a new set of instructions was issued by CSIS in 1989 and subsequently modified by Ministerial direction in April 1991. The revised policy appeared to set clear guidelines for surveillance tape processing and retention. It also established the circumstances in which CSIS would retain surveillance information for transmission to the RCMP. These circumstances were defined as involving a case where the RCMP could not otherwise obtain its own independent evidence and where "exceptional" conditions regarding the seriousness of the information were weighed in conjunction with the potential impact of its use on CSIS sources, methods and "third-party" relations.[38] SIRC pronounced itself satisfied that "the recent policy fills many of the gaps that existed under the early policy."[39]

In sum, the SIRC 1992 study found no "smoking gun" when it came to CSIS-RCMP relations either before the attack on Air India or in the investigative phase up until the time of its report. What it did find were agencies confronted with a wholly unexpected situation that had to translate theoretical policies on information sharing and joint work into on-the-ground collaborative practice. On the whole, they seem to have done so successfully, despite occasional personality conflicts and some rather drawn-out negotiations over access to and use of CSIS information.

What SIRC did discover was a low quality of performance when it came to threat assessments on the part of CSIS. The threat assessments that CSIS issued in the period leading up to the Air India bombing were lacking in specifics and failed to probe alternative threat scenarios, especially when it came to the possibility of terrorist bomb attacks against Air India flights. For example? The SIRC report suggested that the quality of CSIS threat assessment had improved considerably between 1985 and 1992. With the creation of CSIS and the transfer of security intelligence function to that agency in 1984, any potential on the part of the RCMP to use remaining in-house assessment capabilities to challenge CSIS findings was considerably diminished. The RCMP, post 1984, was meant

---

37 ibid., p. 90
38 ibid., p. 87
39 ibid., p. 88

to be a recipient of security intelligence assessment from CSIS, not an independent generator of such intelligence assessments.

Although the SIRC report, in its public redacted version, drew no hard conclusions on the matter, it is clear that deficiencies in intelligence collection, including inadequate physical surveillance coverage and the inability to utilize wiretap surveillance on a timely basis, also affected intelligence reporting before the bombing. Collection and assessment of intelligence are synergistic tasks. Deficiencies in one will feed deficiencies in the other. In the case of the intelligence effort prior to the bombing, it seems clear that CSIS had recognized the threat posed by Sikh extremism in Canada and had been able to identify key targets for surveillance. What the service was not able to do was to get beyond general appreciations of the threat, or to take full advantage of the intelligence gathering operations it had launched. The Air India bombing was the product of an intelligence failure, although it may well fit the profile of the kind of failure that Richard Betts deems inevitable. Air India Flight 182 was not the end result of any significant failure of CSIS-RCMP cooperation.

SIRC'S 1998 Study of CSIS-RCMP Relations

Six years after the completion of its Air India study, SIRC conducted a follow-up investigation of CSIS-RCMP relations. The review was stimulated by on-going concerns on the part of SIRC regarding potential conflict between the services, and was conducted in two parts. Part One studied headquarters-level cooperation between the two services, and was completed in October 1998. A Part Two study, completed the following year, dealt with cooperation at the regional level. Only the Part One study is currently in the public domain in redacted form.

The SIRC 1998 study began with a review of the existing Memorandum of Understanding between the two services, which dated back to 1990. It noted that the Liaison Officer program established to cement relations between the two services and operate as the principal channel for the controlled transmission of information had been a success. But the SIRC study also remarked on the potential impact of the Supreme Court decision of 1991, R. v. Stinchcombe. The actual case heard by the Supreme Court had nothing to do with security intelligence matters, but in adjudicating it, the Supreme Court came down with a very strong statement on the obligation of the Crown to disclose to defence counsel all information in

its possession about a case, so as to "ensure that justice is done."[40] As SIRC related, "The impact of that decision is that all CSIS intelligence disclosures to the RCMP, regardless of whether they would be entered for evidentiary purposes by the Crown, are subject to disclosure to the Courts."[41]

The Stinchcombe decision, in fact, threatened the delicate trade-off at the heart of CSIS-RCMP information sharing. This trade-off involved mechanisms to protect CSIS- originated information when transferred into RCMP hands, via caveats on its use. Seven years after Stinchcombe both services were still mulling over the need for either legislative changes or further revisions to the MOU. Stinchcombe appeared to have the effect of further cementing CSIS's self-image as an intelligence service that collected information for national security purposes, not evidence. It potentially deepened the RCMP's difficulties in sustaining the flow of intelligence, deemed worthwhile as investigative leads, from CSIS. From the vantage point of a review of files between January and August 1997, SIRC restricted itself to a comment that, "while this development has not stopped the flow of information between the two agencies, it has exacerbated some of the concerns on both sides, particularly at the divisional/regional level."[42]

SIRC also expressed an interest in the efforts, led by the RCMP, to create a joint task force to investigate transnational criminal activity. SIRC saw this problem through the prism of potential friction between the two services impacting on information flows. What it really revealed were competing conceptions of the role of the two services in the field of threat assessments. CSIS wished to define its role in transnational crime as providing strategic level assessments, while the RCMP would focus on case-specific issues. That such a division of labour might not be realistic was understood by SIRC, though it had no solution to offer other than a plea to avoid disagreement.[43]

Sidewinder

Unbeknownst to SIRC at the time, the joint transnational criminal project that they had studied in 1997 and reported on in 1998 was a ticking time-bomb. The time-bomb would be project "Sidewinder," a joint RCMP-CSIS

---

40 R. v. Stinchcombe, File 21904, 1991 3 S.C.R. 326

41 SIRC, "CSIS Cooperation with the RCMP, Part 1," October 16, 1998. SIRC Study 1998-04. ATIP version made available by the SIRC ATIP office, p. 9.

42 Ibid., p. 10

43 ibid., p. 21

effort to study the threat posed by Chinese criminal activity possibly related to Chinese state-run foreign espionage. CSIS and the RCMP developed an analytical plan in March 1996 that called for each service to deploy two analysts to form a joint team to produce intelligence briefs on the threat. A "Sidewinder" threat assessment was both long in its production and contentious. A first draft report was prepared in late Spring 1997 but was rejected by CSIS on the grounds that it was "based on innuendo, unsupported by facts." This raised the ire of the RCMP and stalled the project until early in 1998. Work was resumed in January 1998, but disagreements soon emerged again. CSIS took charge of the project and finished a report in January 1999, but it apparently failed to meet full RCMP approval. The internal rancour produced by the project was so great that it led to leaks to the media and members of Parliament, culminating in a series of Globe and Mail articles in September and October 1999 alleging political interference in the handling of the Sidewinder project.

At this point SIRC stepped in with its own study. These were very serious allegations, quite apart from what Sidewinder might tell SIRC about the already sensitive and long familiar issue of CSIS-RCMP cooperation.

SIRC was scathing about the quality of the first draft of the Sidewinder report and essentially agreed with the CSIS decision to shelve it. More difficult to fathom was SIRC's insistence that there was nothing in the history of the project that indicated broader problems between CSIS and the RCMP. In fact, as a joint analytical effort, Sidewinder was unique. The SIRC report itself makes clear the depth of dissatisfaction created by the experience of the project's outcome, especially on the part of the RCMP. The chilling effect was clear in a statement made to SIRC by an RCMP Chief Superintendent that the RCMP would undertake future joint assessments with CSIS, but only "with a much more detailed agreement" and with a "clear working protocol." Such joint assessments, furthermore, "will only be undertaken with CSIS [material redacted] "where both agencies can really benefit from and contribute to a joint project."[44] This was a death knell.

The SIRC study of Project Sidewinder was produced on September 6, 2000. In coming to the defence of CSIS's role in the affair, SIRC muted concerns about the viability of future joint analytical work and reinforced

---

44 SIRC, "Project Sidewinder," SIRC Study 1999-10, September 6, 2000, p. 11. ATIP Version provided by SIRC ATIP office.

a view of CSIS as being the security intelligence assessment top dog. The view was understandable. The CSIS Act had made the Service top dog when it came to national security threat assessments. Nothing in the experience of the history of the service since 1984 suggested it should or could be otherwise. While the service's intelligence collection and assessment performance prior to the Air India bombing had not been stellar, this weakness was seen as a product of immaturity, not of systemic constraints.

What SIRC failed to remark was the idea that Canadian intelligence performance, whether over Air India or Project Sidewinder, might be aided by a degree of competitive intelligence and by a challenge environment. From the very beginning of CSIS's existence, the overwhelming emphasis had been on securing its independence and separate mandate as a civilian security service. Overlap, duplication, and friction with the RCMP were all to be avoided like the plague. Information had to be made to flow between CSIS and the RCMP, but the assumption was that the flow was linear and mostly one-way. CSIS intelligence would flow to the RCMP as needed, primarily to serve as investigative leads to assist the RCMP in its law enforcement mandate. CSIS and the RCMP were to be silos, with an information ramp between them.

The emphasis on the separate and unique mandates of CSIS and the RCMP was understandable, even necessary, but came with hidden costs. They were only to be revealed in the aftermath of the September 11 attacks, when Canada was confronted with security threats from transnational terrorism on a scale never before anticipated.

On the MOU Trail

Efforts to establish both the legal and policy framework for CSIS-RCMP cooperation have consistently focused on the framing of formal documents known as "Memorandum of Understanding" signed by the heads of both agencies. The first of these was laid down in 1984; the most recent dates from September of 2006. They provide, individually and collectively, a template for understanding the aspirations underpinning CSIS-RCMP relations. The history of their composition, to the extent available in the public domain, provides some of the clearest indications of the sources of tension between the two agencies and the distinctive nature of their self-conceptions.

The July 1984 MOU was the prototype.[45] It was focused simply on provisions for the sharing of information between the two agencies, justified by reason of their separate but conjoined legal mandates. Full sharing of information was established as the principle, but hedged by restrictions on the sharing of third party information and on the use of shared information without prior authorisation. The MOU established that "neither CSIS nor the RCMP shall have unrestricted right of access to the operational records of the other agency." The watchword was share, but share as dictated by legal mandates and share with some caution. The 1984 MOU was an accurate reflection of the concerns of the day, based above all in the McDonald Commission's insistence on the need for proper legal regimes to surround security and intelligence work, and for the separation of mandates and powers between a civilian security service and the RCMP.

The 1984 MOU required that the Director of CSIS and the Commissioner of the RCMP develop policy guidelines to implement the memorandum. It was backed up by a robust Ministerial Directive from Bob Kaplan, the Solicitor General, in late July 1984. As the Kaplan directive put it, the organizational separation of CSIS from the RCMP meant that "the formal and informal coordinating mechanisms of a common RCMP structure and the commonality of purpose and outlook which encouraged a high degree of coordination between intelligence and action (enforcement, protection) within the RCMP, will need to be supplanted by other arrangements and understandings between the RCMP and CSIS."[46] The Kaplan directive called on the RCMP to overcome the fragmentation resulting from the separation of security intelligence and law enforcement by building liaison arrangements with CSIS. These liaison arrangements would provide the institutional mechanism for information sharing. Kaplan recognized the potential for overlap of duties and duplication of effort; The Minister also understood that it might not always be possible to demarcate "security intelligence" investigations from "security enforcement" investigations. Close cooperation would have to be the solution.

The major weakness, in retrospect, of the 1984 MOU and the Kaplan directive was in its emphasis on a linear, one-way flow of intelligence

---

45 The July 1984 CSIS-RCMP MOU is included as Appendix A of the Security Intelligence Review 1985," November 16, 1992.

46 Ministerial directive, "Bill C-9 and the Conduct of RCMP Security Responsibilities," dated 10 July, 1984. Bob Kaplan, Solicitor General, to the Director of CSIS, July 239, 1984. Both documents are included as Appendix B of the SIRC 1992 study of Air India, *ibid*.

from CSIS to the RCMP. Not only was CSIS distinguished by way of its monopoly on threat assessments and security intelligence, it was also assumed that the RCMP would have relatively little to contribute of a security intelligence nature from its own sources and knowledge. What this left begging, admittedly for the future, were two issues:

1. whether CSIS could do a fully effective job without security intelligence input from the RCMP (the assumption at the time was yes)

2. how the RCMP could act as a "security enforcement" agency without the benefit of its own intelligence and threat assessments (the assumption was simply that this was CSIS's job)

According to the SIRC, in the first years after separation CSIS and the RCMP signed a total of 17 MOUs, some presumably on more detailed issues of cooperation. The next comprehensive re-framing of the MOU came in 1989-90, when the previous documents were amalgamated into one and revised in April 1990.

The April 1990 MOU marked no radical departure from the principles set out in 1984. The emphasis continued to be on the need for information sharing between two agencies with legally distinct mandates and functions. CSIS was identified as the sole source for national security intelligence, as captured in the wording of the first principle for information exchange:

"the RCMP **will rely** [*emphasis added*] on the CSIS for intelligence relevant to national security offences."[47]

The RCMP's role as informational source was characterized differently: "The RCMP **will provide** *[emphasis added]* to the CSIS information relevant to the CSIS mandate."[48]

An effort was made in the 1990 MOU to draw out the distinctions between CSIS intelligence and RCMP law enforcement work. The MOU noted that

---

47 Memorandum of Understanding Between the Canadian Security Intelligence Service and the Royal Canadian Mounted Police," April 1990., p. 3 Attached as Appendix A to SIRC 1998 Study on "CSIS Cooperation with the RCMP, Part 1"

48 ibid.

while CSIS may from time to time provide the RCMP with information that will have value as evidence, CSIS "does not normally collect information for evidentiary purposes" and that such use would be exceptional and would require prior CSIS approval.[49] Moreover, in a later part of the MOU, categories of information that the RCMP was to share with CSIS drew attention to "detailed case-related information relevant to the security-related responsibilities of the CSIS."[50]

The liaison channels authorized in Bob Kaplan's Ministerial directive of July 1984 were reaffirmed and were tightened up by specific protocols over channels of sharing and dispute resolution and through the creation of a "Senior Liaison Committee," which would have both a policy and an arbitration function.[51]

No revisions occurred to the MOU between April 1990 and September 2006. Some efforts at redrafting were undertaken in 2000 and again in 2002, but went nowhere largely because they were not a high priority for CSIS and failed to satisfy the RCMP, which viewed such efforts as both inadequate and ineffective in addressing contemporary security issues.

It was not until the advent of the Rae investigation into the Air India bombing that both the RCMP and CSIS were stimulated to return to the drafting table. The senior management of both CSIS and the RCMP engaged in on-going discussions between April and October 2005 on the subject of "modernizing" the relationship between the two bodies. The Director of CSIS and the RCMP Commissioner met twice in this period with their senior managers in attendance to personally address this issue. The upshot was a revised CSIS-RCMP MOU, eventually signed on September 29, 2006.

The September 2006 MOU reaffirmed the need for CSIS-RCMP cooperation within the framework of their "distinct yet complementary roles."[52] The relationship between the two agencies was now defined as a "partnership, providing mutual assistance with respect to each other's mandate."[53] As

---

49 ibid., p. 9
50 ibid., p. 10
51 ibid., p. 18
52 Memorandum of Understanding between CSIS and the RCMP, September 29, 2006, p. 1 Courtesy of the Commission of Inquiry into the Investigation of Air India Flight 182, public production # 1374
53 ibid

had been the case throughout the history of the CSIS-RCMP MOUs, the key was finding ways to operationalise the agreement. In this respect, the 2006 MOU did offer something new. In place of an exchange of Liaison officers that had apparently fallen by the wayside, the MOU created a senior level coordinating committee to manage the interaction of the two services on the investigative front, to develop a common terrorist threat assessment, and to develop joint training.

Gone from the 2006 MOU was the language which spelled out the RCMP's "reliance" on CSIS for intelligence and the inference that CSIS would be the main supplier of strategic level information to the RCMP, while the RCMP might contribute tactical, case-oriented information to assist CSIS in its operations.

The thorny issue of transmitting CSIS intelligence into evidence for law enforcement purposes was dealt with in the 2006 MOU by a combination of traditional formulae and new safeguards. The 2006 MOU reflected the now deeply entrenched concern on the part of CSIS about disclosure of their intelligence in the course of judicial proceedings. These disclosure concerns had been heightened by the Stinchcombe decision and had continued to dog CSIS-RCMP relations since 1991. The 2006 MOU asserted two longstanding, but competing principles. One was that CSIS information provided to the RCMP may have "potential value as evidence in the investigation or prosecution of a criminal offence."[54] The other was that CSIS "does not normally collect information or intelligence for evidentiary purposes"—a reflection of its different mandate and different legal grounds for commencing intelligence collection activities against threats to the security of Canada.[55]

The 2006 MOU emphasized the reality of the Stinchcombe environment, in which any information in the possession of the RCMP, no matter what its genesis or intended use in criminal proceedings, might be subject to the laws of disclosure in court. It also invoked the powers of sections of the Canada Evidence Act, generally known as public interest immunity, to provide the government, as needed, with tools to prevent the disclosure of sensitive information in court.

---

54 ibid., para 21
55 ibid

Behind the scenes at least one document prepared by the RCMP during the course of the MOU revision was skeptical about the implications of the use of the public interest immunity clauses (Section 38) of the Canada Evidence Act, arguing that it might involve considerable delay or even the derailment of criminal proceedings. In such a scenario, CSIS-RCMP sharing of intelligence was nullified. An in-house research paper prepared by the RCMP compared disclosure protections available to Canada with those available to its closest intelligence allies. The powers available in Canada were seen as a double-edged sword. The document is worth quoting:

> "When considering the Charter of Rights and Freedoms and the broad right to disclosure in Stinchcombe, section 38 represents a compromise. Information that is injurious to the national interest can still be ordered disclosed if the public interest in disclosure outweighs the public interest in non-disclosure. When section 38 certification is used as a last resort to bar disclosure, key prosecution evidence may then be ruled inadmissible or the charges against an accused may be stayed."[56]

At the end of the process of turning intelligence into evidence lay the prospect of stalled or aborted trails. Only experience, of which Canada was short, would tell. But the process had to be made to work, no matter what the outcome. To that end, the 2006 MOU called attention to the need for joint training and secondments between the two agencies to share knowledge and "enhance understanding of each other's mandate, responsibilities and methodologies."[57] Joint training was new as a concept. Secondments had long been practised but had led to friction between the two services and complaints from CSIS about the under-utilisation of its officers. The 2006 MOU was designed to restore functionality to the secondment process.

The 2006 CSIS-RCMP MOU, like all its predecessors, was nothing more than a piece of paper signed admittedly by the CSIS Director and the RCMP Commissioner. Its test would come with operational experience and with real-world events. It's too soon to say whether the 2006 MOU

---

56 RCMP National Security Support Branch, "Information Sharing Among the 'Five Eyes,' September 6, 2005, pp. 10-11. ATIP version courtesy of the RCMP.

57 CSIS-RCMP 2006 MOU, para. 24

works to achieve its objectives. What can be said is that the objectives themselves are firmly rooted in a substantially altered understanding of the relationship between CSIS and the RCMP. The relationship had moved, over the course of 22 years, from silos to partnership.

The original 1984 MOU described the silo arrangement, with CSIS and the RCMP connected by an informational ramp. CSIS was, in many respects, the tall silo, with its lofty strategic intelligence gaze. The RCMP was the stumpy silo, engaged on in-the-trenches tactical intelligence and case work. The informational ramp flowed one-way.

This system brought no benefits at the time of the Air India terrorist attack. It is impossible to say with certainty whether a different system could have prevented, through better intelligence work, the attacks on Air India , or it could have netted the main instigators in the aftermath of the attack.

Lessons were not quickly learned about the inadequacies of the post 1984 system of domestic intelligence and security that Canadians built for themselves. Lessons were not learned because expectations were relatively low concerning the role and value of intelligence in counter-terrorism, because of the assumption that the attacks on Air India had come at an unfortunate moment of "immaturity" on the part of CSIS and the new structures of security intelligence, and because we had invested heavily in the notion of the distinctiveness of the intelligence and law enforcement functions. We had built our own conceptual "Chinese Wall" to separate security intelligence and law enforcement.

A variety of factors worked to solve the "immaturity" problem: time, experience, new personnel intake, new leadership, the prodding of SIRC and one-off advisory studies with that conducted by Gordon Osbaldeston. Perhaps the experience of Air India was a prod, but if so it is hard to document.

Different expectations about the intelligence function and a re-thinking of the intelligence-law-enforcement relationship would only emerge in a post 9/11 environment. This can be construed as a result of a failure to learn lessons directly from the Air India disaster. But it was also a matter of evolution, experience, and a growing distance from the shaping experience of scandal and disillusion with the performance of the RCMP security service that had been the original impetus for the creation of

CSIS in 1984. Above all, the kind of relationship between CSIS and the RCMP imagined in the 2006 MOU was a direct product of the post 9/11 environment. That environment was shaped by a much greater sense of threat to national security than anything that transpired surrounding the advent of Sikh extremism and the bombing of Air India. With a greater sense of threat came a much greater sensitivity to the intelligence function and to the significance of CSIS-RCMP relations.

Post 9/11 Developments

The Al Qaeda suicide attacks on targets in the United States on September 11, 2001 came as a shock and surprise to the Canadian intelligence community. Those attacks plunged Canada into a crisis atmosphere. In their immediate aftermath, the United States declared a global "war on terror" and Canada signed as a NATO member state an unprecedented Article V declaration of collective defence against attack. Fears of an imminent second wave of terrorist strikes sparked an intensive hunt for potential underground Al Qaeda cells throughout North America. The Canadian government scrutinized its own resources to deal with the threat of global terrorism and began a process of significant national investment in upgraded security capabilities as well as the development of new legal powers.

Both the RCMP and CSIS were major beneficiaries of new spending on national security, packaged in a "national security" budget announced by then Finance Minister Paul Martin in December 2001. This financial largesse reflected a sense of the lead role that both agencies would have to play in the face of an unprecedented and unexpected threat environment.

More significant than the budget outlay was the framing of Canada's first anti-terrorism act, passed into law in December 2001. Bill C-36 criminalised terrorism, and added new clauses to the criminal code. It created or expanded new legislative mandates for elements of the Canadian intelligence community such as the Communications Security establishment and FINTRAC (Financial Transactions Reports Analysis Centre). It significantly amended the Official Secrets Act, renamed as the Security of Information Act. The Attorney General acquired new powers with regard to the issuance of "public interest" immunity certificates. There is no doubt that the anti-terrorism act lived up to its billing as an "omnibus" piece of legislation.

It is important to note that the Anti-Terrorism Act involved no change to the mandate of either the RCMP or CSIS. No new "powers" were granted to either agency, as was frequently suggested in the media. But equally it is the case that the criminalization of terrorism broadened the scope of RCMP national security investigations, while the greater threat posed by global, transnational terrorism in the post 9/11 era fundamentally affected the intelligence priorities of CSIS, as well as the Communications Security Establishment and many other elements of the Canadian security and intelligence community.

The first phase of Canadian counter-terrorism policy after 9/11 was essentially reactive and dictated by the demands of a crisis environment. The government of Canada concentrated its energies on injections of money to boost national security capabilities, new legislation, and the Canada-US relationship, particularly in terms of border security and trade.

Reactive policy was ultimately accompanied by more strategic and long-range decision-making. As the events of 9/11 and its aftermath were absorbed and reflected on, the federal government began to conceptualise the role of intelligence differently, made major alterations to institutional structures, and set out a comprehensive strategic vision. This work accelerated with the ascension of the Paul Martin government in December 2003.

Two key themes emerged in this second wave of government reaction to the new post 9/11 security environment. One was the concept of intelligence as a "first line of defence." The other was the emergence of a doctrine of "integrated" national security practice. Both would provide the underpinnings for the declaration of CSIS-RCMP partnership framed in the CSIS-RCMP 2006 MOU.

The primacy of intelligence as a tool of national security policy was reflected in the National Security Policy document issued in April 2004. This document contained a statement never before expressed in the history of government strategic doctrine:

"Intelligence is the foundation of our ability to take effective measures to provide for the security of Canada and Canadians. To manage risk effectively, we need the best possible information about threats we face and the intentions, capabilities and activities of those who would do us harm. The best decisions regarding the scope and design of security programs, the allocation of resources and the deployment of assets cannot be made unless decision makers are as informed as possible." [58]

This new concept of the role of intelligence substantiated previous decisions taken on fiscal outlays. But it also operated alongside a determination to alter the institutional setting for intelligence work in Ottawa, a change based on an appreciation that the older model of "organizational silos" had to be surmounted. The National Security policy called attention to a series of measures already undertaken to ensure more effective intelligence work. This included the creation of a new senior Ministry, the Department of Public Safety and Emergency Preparedness Canada, the establishment of the post of National Security Advisor to the Prime Minister, and, as a focus for collective threat assessment, the construction of the Integrated Threat Assessment Centre (ITAC). ITAC's design was meant to symbolize a new way of doing intelligence in Ottawa. It would be based on collective intelligence input from a wide range of government departments and would circulate its product to "all who require them." [59] As a sign of the, at least symbolic, place that ITAC would have at the heart of government analysis, it was to report to both the Minister of Public Safety and the National Security Adviser. ITAC was also built as a new mechanism to ensure CSIS-RCMP "partnership," Not only were the two agencies seen as the main contributors to ITAC, the Centre itself was to be located in CSIS, but headed by a senior official seconded from the RCMP.

Integration was a complementary theme, highlighted as well in the 2004 National Security Strategy. The strategy paper had this to say about the importance of integration:

"The increased complexity of the threats facing Canada requires an integrated national security framework to address them. It is critical for

---

58 "Securing an Open Society: Canada's National Security Policy," April 2004, p. 15. Available online at www.pco-bcp.gc.ca

59 ibid., p. 18

our key security instruments to work together in a fully integrated way to address the security interests of Canadians."[60]

In addition to the creation of PSEPC and the post of National Security Adviser, the document also called attention to the establishment of a standing Cabinet committee on "Security, Public Safety and Emergency Preparedness."[61]

While the National Security Strategy was designed with a wider advocacy in mind, it spoke to issues crucial to change in the CSIS-RCMP relationship. The concept of "partnership" enshrined in the 2006 MOU was a re-statement of the concept of "integration" expressed in the 2004 strategy. Like the 2006 MOU, the 2004 strategy paper represented a policy departure, and laid down a new conceptual framework. Implementation of the strategy, especially in terms of achieving effective integration, remains a work in progress. Neither the 2006 MOU nor the 2004 strategy document were conceived of as efforts to learn lessons from Air India. In practice, both policies captured lessons that had to be learnt, but also had to wait until a different climate of threat appeared after 9/11.

Conclusions

The security intelligence system erected in Canada in 1984 with the creation of CSIS was a product of the immediate experience of scandal and poor performance of national security functions by the RCMP Security Service. In separating the security intelligence function from the security enforcement function, the Canadian government looked to fix the problems of the past and did so by way of a familiar Canadian institutional pattern, one rooted in a concept of intelligence and law enforcement "silos" with distinct functions and mandates. The Canadian security and intelligence community was historically decentralised, with only weak central coordination and leadership. This decentralized system was effectively reinforced with the creation of CSIS and the separation of powers and mandates between CSIS and the RCMP. Though the possibility of problems in cooperation between the two agencies was anticipated from the outset, a solution was looked to in the construction of formal Memoranda of Understanding between the agencies, backed by Ministerial directives. What the Canadian system did, in 1984 and

60 ibid., p. 9
61 The Cabinet committee has since been altered to one dealing with "Foreign Affairs and Public Safety."

after, was in effect to construct a made-in-Canada version of a "Chinese wall" between the RCMP and CSIS and then require the two agencies to surmount the wall through cooperation in information sharing and investigative practices. Effecting cooperation was largely left to the leadership and rank and file of the two agencies, with only occasional probes from outside, usually mounted by the Security Intelligence Review Committee.

At no point in the aftermath of the Air India bombing was the attack officially understood as an intelligence failure. The Seaborn report, the first postmortem, instead emphasized minimalist expectations of the role of intelligence in the face of terrorist threats. The much more substantial study of Air India embarked on by SIRC in the early 1990s, did call attention to weaknesses in CSIS intelligence, but shied away from calling Air India an intelligence failure *tout court*. The failure to call a spade a spade in public had the effect of reducing attention to the need to learn lessons from the performance of the security and intelligence community.

Although the CSIS-RCMP Memorandum of Understanding was revised and tinkered with between its initial composition in 1984 and 2002, no major, systemic changes in the relationship between the two agencies occurred. Throughout most of this 18 year period, they continued to operate as "silos" in a decentralized system. This was not primarily a product of bureaucratic rigidity, institutional insularity, or failures of leadership. It was a product of what was wanted.

What went unrecognized prior to the advent of the 9/11 era was that CSIS-RCMP cooperation had at its heart the requirement for an effective capacity for intelligence gathering, assessment and dissemination on the part of both agencies. Instead, these classic components of the intelligence cycle were deemed to be exclusively a CSIS function, and the RCMP was situated as a consumer of intelligence, rather than a student of it. Such a precise, functional division of labour was unrealistic, bound to cause problems, and had the effect of robbing CSIS of a good understanding of RCMP methodology and of robbing the RCMP of a good appreciation of how best to use intelligence for investigative purposes. Moreover, the functional division of labour laid down in 1984 robbed the system of the benefits of competitive intelligence. As Judge Richard Posner has reminded us, systems that display a capacity for competitive

intelligence ensure better diversity of insight and act as a brake on regnant preconceptions. [62]

This is not to say that the Air India disaster could have been averted by a different intelligence system, or a different division of labour between CSIS and the RCMP. Here, the admonishment of Richard Betts with regard to the inevitability of intelligence failure is a useful caution.

What can be said with confidence is that the inadequacies of the 1984 system were only fully appreciated in the aftermath of the 9/11 attacks. The effort to correct these inadequacies after 9/11 were extensive and significant, and included a new understanding of the lead role of intelligence, a new definition of a "partnership" between CSIS and the RCMP, reflected in the 2006 MOU, and greater efforts at institutional and strategic integration to overcome the prior history of the silo effect.

The temptation might be to say that changes effected in the Canadian security and intelligence system after 9/11 have resulted in a belated learning of lessons left unaccomplished after Air India. But there are two problems with this. One is that the effort to learn lessons directly from Air India was real and sustained but its limitations have to be understood in their historical context. It took the much greater domestic and international shock of the 9/11 attacks to produce an earthquake effect in the Canadian intelligence system. The 9/11 attacks and the advent of global, transnational terrorism as a principle national security threat forced change in a way that Air India failed to do.

A second problem with taking comfort from the recent changes is that they are recent and remain, in many respects, to be fully tested. This is especially true of the 2006 MOU and its invocation of "partnership." As the report of Justice O'Connor into the case of Maher Arar reminds us, there remains a great deal of work to be done to ensure that both CSIS and the RCMP respect their distinct mandates while "working together in a cooperative and integrated manner."[63] The days when that distinctiveness seemed uncomplicated and when CSIS and the RCMP were left alone to figure out ways to surmount their Chinese wall are behind us. What is ahead is a new definition of intelligence partnership and a new and more sustained monitoring, both internal and external, of CSIS-RCMP

---

62 Richard A. Posner, Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11 (New York: Roweman and Littlefield,2005), p. 155

63 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Analysis and Recommendations, especially Recommendation #1, pp. 312-15.

relations. It is also worth hoping that what is ahead for Canada is a more sustained commitment to a study of security and intelligence problems that will continue on after the Air India Inquiry closes its doors and issues its report.

The Way Forward:

The greatest challenges to the achievement of CSIS-RCMP cooperation in the future are the need to fashion a true "partnership" and to engage in genuine integration of national security activities. Progress towards these goals will need to be encouraged and scrutinized using the existing mechanisms of accountability and review available with the Government of Canada system. Parliament, the Minister, existing review bodies, both internal and independent, will all need to play a role. There will be continued work for the Office of the Auditor General in monitoring the effectiveness of CSIS and the RCMP's pursuit of partnership and integration. Nothing new need be built into the system. Instead, what is required is sustained attention and an appreciation that partnership and national security integration are not easy tasks, and not ones to be left to the agencies themselves to accomplish on their own—as was the case for much of the time covered by this report.

This report has found that one of the systemic deficiencies in intelligence, that broadly affected CSIS-RCMP capabilities and cooperation, was a product of a too rigid definition of roles and functions when it came to intelligence production. The system created in 1984 and sustained throughout the period down to the 9/11 attacks was premised on a notion of CSIS as intelligence producer and the RCMP as intelligence consumer. This notion robbed the Canadian system of a capacity for competitive intelligence judgments, robbed the RCMP of a capacity to generate intelligence to apply to their national security investigative function, or to use intelligence well, and made difficult the inter-connection between the two services. In an understandable effort to accomplish the objectives of the McDonald Commission in establishing a civilian security intelligence function, we produced an institutional environment which made sharing and cooperative endeavours more difficult than they needed to be. The sorry history of the Sidewinder affair is a testament to this problem.

With the advent of a new appreciation of the significance of intelligence, post 9/11 and a recognition that intelligence needs to be a product and manifestation of a more integrated national security system, there is an

opportunity to learn from our history and our errors. But creating a high quality, integrated national security intelligence product will take work. It will require talent, resources, and a cultural shift within the security and intelligence community towards sharing and mutual appreciation of the contributions of a wide variety of agencies. A true competitive intelligence environment requires a difficult to achieve combination of competition, respect, sharing and accommodation to distinct outlooks.

What might be done to help bring such an intelligence environment into being? This question is worthy of further and sustained thinking. But two suggestions would involve the weight of critical scrutiny, applied from different angles. The ultimate test of an intelligence product is in part its veracity, but also its usefulness and acceptance by senior decision-makers. One way to challenge the production of integrated, high-quality intelligence assessments would be to put them to the test of having to perform as a regular, high-level product for Cabinet. Another way to put the intelligence product to a test, and to broaden the competitive intelligence environment, would be to submit some intelligence assessments to review and scrutiny by a panel of security cleared expert advisers. In both cases the achievement of integration and partnership in intelligence production is shifted as a burden from the shoulders of CSIS and the RCMP alone.

CSIS and the RCMP are public institutions. Their personnel are recruited from the public, and as institutions they are ultimately accountable to the public. Their effectiveness is a matter of great public interest. If the public has high expectations of the performance of CSIS and the RCMP, it is also important that the public be in a position to realistically scrutinize and critique the conduct of these principal national security institutions. Such a capacity is made intrinsically difficult by the secrecy that must surround national security operations. Yet there is a legitimate public need to know. The Air India Inquiry reflects that public right.

The lessons that are learned from the inquiry into Air India must be lessons learned not only by government institutions but by the public at large. To accomplish this, there is a need to expand the potential of public knowledge and to make sure that it is sustained beyond the life of the Commission itself. The public needs to see that the inadequacies of past practices of intelligence production and CSIS-RCMP cooperation have been resolved. To that end, there is a requirement for a greater effort

on the part of the Government of Canada to inform the public about the on-going operations of its national security agencies and progress in achieving the objectives of partnership and integration. There is also a need for a greater public research capacity into the history of our national security institutions. The Government of Canada should be encouraged to create a dedicated funding mechanism to encourage in-depth research and writing on the Air India disaster and on other cases of terrorist threats to Canadian society. The Government should also be encouraged to release to the National Archives for open research all historical documents relating to the Canadian response to Sikh extremism, with exemptions applied only where strictly necessary on national security grounds. We need to open up both our historical and our present national security activities to greater and more informed public scrutiny. Only when we do so will we have a baseline for gauging success in the complex world of security intelligence and enforcement.

Wesley Wark

Wesley Wark is an associate professor at the University of Toronto's Munk Centre for International Studies, where he has taught since 1988. He is also a visiting research professor at the University of Ottawa's Graduate School of Public and International Affairs. He earned his degrees from Carleton University (BA), Cambridge (MA) and the London School of Economics (Ph.D). Prior to joining the University of Toronto, he held teaching appointments at McGill University and the University of Calgary.

Professor Wark is one of Canada's leading experts on intelligence and national security issues. He is a Past-President of the Canadian Association for Security and Intelligence Studies (1998-2000 and 2004-2006). He serves on the Canadian government's Advisory Council on National Security and the Advisory Committee to the Canada Border Services Agency.

He is completing a book on the history of Canada's intelligence community in its formative years from the end of World War two to the height of the Cold War, and a study of contemporary Canadian national security policy and counter-terrorism. His most recent scholarly publications include a special issue of the International Journal, published by the Canadian Institute for International Affairs/Canadian International Council, devoted to the subject of "Security in an Age of Terrorism," (Winter issue 2004/05) and an edited volume, Twenty-First Century Intelligence (London: Routledge, 2005). A new edited collection, Understanding Secret Intelligence, co-edited with Richard Aldrich and Christopher Andrew, is due out later in 2008.

He is co-director, with Mel Cappe, of a major research project funded by the Institute for Research on Public Policy on "Security and Democracy."

In 2006, he completed a study of key research issues in national security and human rights for the Canadian Human Rights Commission and served as an expert court witness on the history of Canada's official secrets legislation. In 2008 he completed an expert witness report on Canada's Marine Transportation Security Clearance Program, which is before the Federal Court.

Professor Wark is a frequent commentator in the media on security and intelligence issues and is a regular book reviewer for The Globe and Mail.

THE ROYAL CANADIAN MOUNTED POLICE AND THE CANADIAN SECURITY INTELLIGENCE SERVICE

A COMPARISON OF OCCUPATIONAL AND ORGANIZATIONAL CULTURES

Paper presented by

Jean-Paul Brodeur
Director
Centre international de criminologie comparée
Université de Montréal

to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182

Introduction[1]

The purpose of this study paper is to present a comparative analysis of the occupational and organizational cultures of the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP). CSIS is a civilian agency, and none of its members work in uniform. In contrast, the RCMP was first created in 1873 as a military force – the North West Mounted Rifles[2] – and the majority of its members still operate in uniform. It would be interesting to compare a civilian agency such as CSIS and a uniformed policing organization in all their aspects. However, such a comparison would be only of academic interest to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182. The Commission's mandate, as its title makes clear, is to inquire into the *investigation* of the bombing of Air India Flight 182. The investigative arm of the RCMP (and other police forces) and CSIS carried out this investigation, so I propose to focus on the respective cultures of both agencies *as they came into contact* in the context of a particular investigation and other overlapping duties.

My study relies on open sources. There is both a dearth and an abundance of such sources. A recent review of the research literature on policing has shown that criminal investigation was the least researched subject in the field of policing.[3] When criminal investigators are studied, researchers focus less on their professional culture than on their role in criminal prosecutions.[4] Because the work of security intelligence agents is shrouded in secrecy, their professional culture is generally not the object of empirical study. The academic literature on spying generally focuses

---

1 Jean-Paul Brodeur holds a Ph.D in philosophy from the University of Paris and a Masters of Criminology from the University of Montreal. He is a former student of the Paris *École pratique des hautes études* (Oriental Languages). He is presently a full professor at the *École de criminologie* of the *Université de Montréal* and the director of the *Centre international de criminologie comparée* at the same university. Opinions expressed are those of the author and do not necessarily represent those of the Commission or the Commissioner.

2 Jean-Paul Brodeur, "*La Gendarmerie Royale du Canada*" in *Les Cahiers de la Sécurité intérieure, Gendarmeries et polices à statut militaire* (Paris: Institut des Hautes Études de la Sécurité intérieure, La Documentation française, 1992) 173 at 175.

3 U.S., National Research Council, Committee to Review Research on Police Policy and Practices, Committee on Law and Justice, Division of Behavioral and Social Sciences and Education *Fairness and Effectiveness in Policing; The Evidence* (Washington, DC: The National Academies Press, 2003) at chapter 1.

4 Andrew Sanders, "From Suspect to Trial" in M. Maguire, R. Morgan and R. Reiner, eds., *The Oxford Handbook of Criminology* (Oxford: Oxford University Press, 1994) 773 (Sanders' classic study is tellingly entitled "From Suspect to Trial."); Jean-Paul Brodeur "L'enquete policiere" in *Criminologie* (Montreal: Les Presses de l'Universite de Montreal, 2005) 39.

on historical research.[5] For glimpses into the "wilderness of mirrors,"[6] one has to rely on disgruntled spies with an axe to grind,[7] biographies,[8] the published work of investigative journalists[9] or the occasional memoirs of bureaucrats with a reputation to save.

It is precisely because of this dearth of first hand sources on the occupational and organizational cultures of criminal investigation units and security agencies that we have to skim through various bodies of literature in order to glean elements that can allow us to complete the picture. The field that we have to cover is relatively broad, but there is a wealth of government literature, including reports of special commissions of inquiry and task forces, reports and written proceedings of parliamentary committees,[10] annual reports of the bodies that review CSIS and the RCMP, and the reports of these two agencies themselves. As my paper will show, I have covered these sources nearly exhaustively. I found one source to be particularly rich – the annual reports and *ad hoc* studies[11] of the Security Intelligence Review Committee (SIRC).[12] SIRC investigated the bombing of Air India Flight 182[13] and offered to make all

---

5 Christopher Andrew, *Her Majesty's Secret Service* (New York: Viking Press, 1986); Christopher Andrew and Oleg Gordievsky, *KGB - The Inside Story* (London: Hodder & Stoughton, 1990); Alain Dewerpe, *Espion: Une Anthropologie historique du secret d'État contemporain* (Paris: Gallimard, 1994).

6 D.C. Martin, *Wilderness of Mirrors* (New York: Harper and Row, 1980).

7 Allen Dulles *The Craft of Intelligence* (New York: Signet Books, 1965); V. Marchetti and J.D. Marks, *The CIA and the Cult of Intelligence* (New York: Alfred A. Knopf, 1974); William Colby, *Honorable Men: My Life in the CIA* (New York: Simon and Schuster, 1978); Mike Frost and Michel Gratton, *Spyworld* (Toronto: Doubleday, 1994).

8 Thomas Powers, *The Man Who Kept the Secrets: Richard Helms and the CIA* (New York: Alfred A. Knopf, 1979); Tom Mangold, *Cold Warrior: James Jesus Angleton: The CIA's Master Spy Hunter* (London: Simon and Schuster, 1991).

9 John Sawatsky, *For Services Rendered: Leslie James Bennett and the RCMP Security Service* (Toronto: Doubleday, 1982); Richard Cléroux, *Official Secrets: The Story behind the Canadian Security Intelligence Service* (Toronto: McGraw-Hill Ryerson, 1990); Andrew Mitrovica, *Covert Entry: Spies, Lies and Crimes Inside Canada's Secret Service* (Toronto: Random House, 2002).

10 For example, see Canada, Senate, *A Delicate Balance: A Security Intelligence Service in a Democratic Society: Report of the Special Committee of the Senate on the Canadian Security Intelligence Service* (Ottawa: Supply and Services Canada, 1983); *Terrorism: Report of the Senate Special Committee on Terrorism and Public Safety* (Ottawa: Minister of Supply and Services Canada, 1987); and *Terrorism: Report of the Second Special Committee of the Senate on Terrorism and Public Safety* (Ottawa: Minister of Supply and Services, 1989).

11 For instance, on December 9, 1994, the Security Intelligence Review Committee released an extensive report to the Solicitor General of Canada: Security Intelligence Review Committee, *The Heritage Front Affair: Report to the Solicitor General of Canada* (Ottawa: Security Intelligence Review Committee, 1994).

12 SIRC's annual reports cover the fiscal year (for example, 2006-07). Over the years, the reports have carried different titles – for example, *Annual Report 1994-95*; *An Operational Audit of CSIS Activities: Annual Report 1996-1997*; and *SIRC Report 2002-2003: An Operational Review of the Canadian Security Intelligence Service*. This paper refers to all these annual reports as follows: SIRC *Annual Report [fiscal year]* – for example, SIRC *Annual Report 1994-95*.

13 SIRC *Annual Report 1991-92*.

its findings available to a royal commission if the government convened one.[14] More important for the purposes of this study, SIRC presided over the transition from the RCMP Security Service to the creation of CSIS and later assessed the co-operation by CSIS with the RCMP.[15] In a significant way, the annual reports of SIRC chronicle the repeated meeting of the professional cultures of CSIS and of the RCMP.

This paper has four parts. First, I provide **context** for the analyses of the occupational and organizational cultures of CSIS and the RCMP. Second, I discuss the **main contrasts** between these two cultures. Third, I examine more briefly a series of other differences. Last, I provide a summary of the contrasting features of CSIS and the RCMP and elaborate on some of them. I conclude with suggestions for the Commission to consider.

1. CULTURES IN CONTEXT

Here, I provide the context for discussing the respective occupational and organizational cultures of CSIS and the RCMP. First, I will refer to the 1985 bombing of Flight 182 and related attempts at terrorism that form the backdrop of this study. Second, I will then review the transition from the RCMP Security Service to CSIS and the evolution of the relationship between the two agencies. Although it is not the purpose of this paper to study the history of both agencies, it is crucially important to be aware that CSIS had not even been in existence for a year when Air India Flight 182 exploded over the Atlantic on June 23, 1985. As CSIS only began its formal existence on July 16, 1984, and it is highly unlikely that by June 1985 it had developed its own professional culture. Contrasting CSIS with the RCMP in 1985 is premature, as CSIS was at that time only a second incarnation of the RCMP Security Service and had yet to elaborate its own independent character.

In my view, the Commission should explore the hypothesis that the Air India investigation was irremediably bungled in its initial stages because of the investigative chaos that was consequent upon the transition from the RCMP Security Service to the newly created CSIS (wholly staffed with recycled RCMP Security Service personnel), rather than because of a difference between police and security intelligence agency professional cultures. I will come back to this suggestion in my concluding remarks.

---

14 SIRC *Annual Report 1994-95* at 23.

15 SIRC *Annual Report 1997-98* at 27-32, referring to SIRC Report #101 (CSIS Cooperation with the Royal Canadian Mounted Police – Part I); SIRC *Annual Report 1998-99* at 20-24, referring to SIRC Report #108 (CSIS Cooperation with the RCMP – Part II).

1.1 The Bombing of Air India Flight 182 and Related Events

Air India Flight 182 exploded while airborne, and everyone on board – 329 persons – died. On the same day, a suitcase bomb detonated at Tokyo's Narita Airport, killing two baggage handlers as they were unloading CP Air Flight 003 from Vancouver. In addition to these high profile incidents, Santokh Singh Khela and Kashmir Singh Dhillon were convicted in Quebec of conspiracy to commit murder in relation to an attempt to recruit persons to help them blow up an Air India plane in New York in the fall of 1985. They were sentenced in 1986 to life imprisonment (I return later to this lesser-known incident).

Despite extensive investigative efforts by the RCMP and CSIS, the bombing of Air India Flight 182 and the explosion at Narita Airport remained unsolved. In the years immediately following the 1985 attacks, there was frequent criticism of the agencies conducting the investigation for not bringing any suspect to trial. There were no criminal proceedings directly related to Flight 182 until April 2003, when three members of the Vancouver Sikh community – Ajaib Singh Bagri, Ripudaman Singh Malik and Inderjit Singh Reyat – were accused of conspiracy to bomb Air India planes. Reyat pleaded guilty to manslaughter, but Bagri and Malik were acquitted.

SIRC had the mandate to oversee CSIS, and SIRC's first reports frequently referred to the Air India bombings.[16] SIRC decided in December 1988 to conduct an inquiry into the role of CSIS in the Air India investigation, but the Government opposed SIRC's decision, arguing that an inquiry could hinder the RCMP investigation of the Air India bombings and the course of justice.[17] In May 1991, Inderjit Singh Reyat was tried for the Narita bombing and convicted of manslaughter for making the bomb and helping others to make it.[18] This development opened the way for SIRC's inquiry, which was then held during 1991 and 1992. SIRC's inquiry report was "a long one and much of its content must remain classified."[19]

---

16 SIRC refers to the Air India bombings in several places in its annual reports: SIRC *Annual Report 1985-86* at 17; SIRC *Annual Report 1986-87* at 28); SIRC *Annual Report 1987-88* at 1, 30; SIRC *Annual Report 1988-89* at 5, 20; SIRC *Annual Report 1989-90* at 17); SIRC *Annual Report* 1990-91 at 17; SIRC *Annual Report 1991-92* at 5-14 (the report on SIRC's own Air India inquiry); SIRC *Annual Report 1994-95* at 23 ("Should the Government of Canada see fit to convene a Royal Commission to investigate all dimensions of the terrorist act, we will offer our complete cooperation.").

17 SIRC *Annual Report 1990-91* at 17-18.

18 Reyat would plead guilty to a similar charge in relation to the bombing of Air India Flight 182 in 2003.

19 SIRC *Annual Report 1991-92* at 5.

The content of the report that could be publicly divulged is published as part of a SIRC report.[20] The inquiry report addresses several issues relating to the respective professional cultures of CSIS and the RCMP and also discusses the co-operation of these agencies in the Air India investigation from 1985 to 1991, so it not only provides context for this paper but is also a good introduction to our topic.

A. *Threat assessments.* Bolan[21] mentions that CSIS issued no less than 15 threat assessments to the RCMP in the months preceding the Air India bombings, making it seem that their planning took place under the nose of CSIS. Actually, CSIS was tasked to investigate Sikh extremism because of the impending visit to Canada of Indian Prime Minister Rajiv Gandhi. The Government of India warned Canada about threats to India's national airline. These warning were not initially addressed to CSIS, but to the Department of External Affairs or the RCMP. The RCMP asked CSIS to provide a threat assessment on the basis of these warnings. CSIS confirmed on June 6, 1985, that the threat to Indian interests in Canada, including Air India, was high, but that it had no specific information about an impending attack against the airline. After Rajiv Ghandi's departure from Canada on June 17, CSIS relaxed its surveillance, and less than a week later, on June 23, the bombings occurred. The CSIS surveillance project had not produced any actionable intelligence about the conspiracy against Air India.[22]

B. *Intelligence follow-up.* This conclusion about a lack of actionable intelligence can be questioned. On June 4, 1985, a CSIS agent followed a person under surveillance to Vancouver Island, where the person met with Inderjit Singh Reyat, later revealed to be a bomb expert. They drove to a remote area and conducted a noisy experiment that the agent mistook from a distance as the discharge of a rifle. CSIS investigators warned the RCMP the following day, but neither agency undertook to follow up this lead by conducting a physical search to verify whether the noise was actually a rifle shot. The RCMP did conduct such a search after the Air India bombings, and the search produced evidence that an explosive device may have been tested on the site. Even then, this finding was not followed up by any analysis, nor was the targeting of the two individuals renewed.[23]

---

20 *Ibid.* at 5-14.
21 Kim Bolan, *Loss of Faith: How the Air India Bombers Got Away with Murder* (Toronto: McClelland & Stewart, 2005) at 48.
22 SIRC *Annual Report 1991-92* at 8-9.
23 *Ibid.* at 8.

C. *Cooperation between CSIS and the RCMP.* SIRC's conclusions about the level of co-operation between CSIS and the RCMP were laced with ambiguities that would become the hallmark of SIRC's future *public* assessments. SIRC found no general evidence of "conflict or lack of co-operation" between the two agencies and downplayed "personality differences" and "one serious dispute" involving "an acrimonious exchange between two senior officers of the agencies" after the tragedy. All of this certainly appeared to contradict SIRC's overall assessment.[24] The contentious issue was that some CSIS agents performed their inquiries as though they were criminal investigators and competed with the RCMP to solve a case that fell squarely within the criminal investigation mandate of the RCMP. According to SIRC, this tension was generated by the lack of instructions from CSIS headquarters clarifying the CSIS mandate *vis-à-vis* the RCMP mandate to conduct criminal investigations, and the failure to set CSIS policies about sharing intelligence with the RCMP.[25] This explanation is somewhat surprising, since a memorandum of understanding (MOU) between CSIS and the RCMP was signed on July 17, 1984, and coincided with the birth of CSIS.[26] Memoranda of understanding between CSIS and the RCMP were also exchanged in 1986-87 and in 1989-90.[27] This situation highlights the problem of disseminating instructions from the headquarters of both agencies to their regional offices and of ensuring that the instructions are applied in the field. It remains to be seen whether the RCMP/CSIS MOU signed on September 29, 2006, will fare better than its predecessors.

D. *The destruction of criminal evidence.* Competition between CSIS and RCMP investigators was not the only source of friction between the two agencies. CSIS was reluctant to expose its files on Sikh extremism to the RCMP. CSIS argued that these files had been developed for intelligence, not evidentiary, purposes. The matter was resolved after "lengthy negotiations" that determined conditions on the subsequent use by the

---

24 *Ibid.* at 10.

25 *Ibid.*

26 The *Honourable Bob Rae, Lessons to Be Learned, the report of the Honourable Bob Rae, Independent Advisor to the Minister of Public Safety and Emergency Preparedness, on outstanding questions with respect to the bombing of Air India Flight 182 (Ottawa: Air India Review Secretariat, 2005), chapter 4:* "The RCMP and CSIS: Background"[*Rae Report*].

27 "The Solicitor General has provided us with a copy of a memorandum of understanding between the RCMP and CSIS, consolidating a number of arrangements for cooperation and for sharing services and administration:" SIRC *Annual Report 1986-87* at 27. "The Service's relations with the RCMP were put on a more systematic footing in 1989-90 with the signature of a Memorandum of Understanding (MOU) between the two. The MOU does not add anything new, but it brings together in one coherent document a number of ministerial directions issued to both agencies over the years:" SIRC *Annual Report 1989-90* at 16.

RCMP of the CSIS files. SIRC[28] found no evidence that access to available CSIS intelligence relevant to the RCMP Air India investigation was "**unreasonably**" denied to the Force. There was, however, one serious practical problem that could not possibly be solved. Between March and July 1985, CSIS erased three-quarters of the 200 or so audiotapes recording conversations of its investigation's principal target.[29] The destruction of these tapes after their content had been summarized and logged was apparently in conformity with CSIS policy – a policy that SIRC later judged to be seriously deficient.[30] Furthermore, an instruction was issued to CSIS **three months before it came into being**, which removed from the Service (whose members were deprived of law enforcement powers) the capacity to collect and preserve tapes as criminal evidence. However, another instruction compelled CSIS to retain tapes containing incriminating passages for one year. For reasons said by SIRC to be unclear, the regional offices of CSIS chose to ignore this second instruction.[31]

The erasure of the tapes uncovers two problems. First, some of the information contained in the taped conversations was destroyed, as it may not have been logged in the written summaries of the tapes. Second, it shows the gap between *intelligence*, which may be summarized and stored in any convenient way for future analysis, and *evidence*, which ought to be preserved in its original form for later production in court.[32] The difference between intelligence and evidence is a critical issue that will be discussed in detail in subsequent parts of this paper.

This review of the findings of SIRC's inquiry into the investigation of the Air India bombings and into the cooperation between CSIS and the RCMP already highlights many of the issues that I will focus on, particularly the difference between intelligence and evidence and the contrasting attitudes of agencies, depending on whether they are

---

28 SIRC *Annual Report 1991-92* at 10.

29 A CSIS agent revealed to *The Globe and Mail* in an interview that he had destroyed hours of audiotaped interviews with two confidential sources who belonged to the Vancouver Sikh community instead of handing the tapes to the RCMP. He feared that the RCMP would reveal the identity of the sources by summoning them to testify in public court proceedings. This agent said that "his actions were the result of a fierce turf war between the RCMP and CSIS" and that in its early stages CSIS's investigation "was so badly bungled that there was a near mutiny by CSIS officers involved in the probe:" Andrew Mitrovica and Jeff Sallot, "CSIS agent destroyed Air-India evidence," *The Globe and Mail* (January 26, 2000) A1-A2. This latter testimony on the intensity of the frictions between CSIS and the RCMP contrasts with SIRC's reassuring conclusions.

30 SIRC *Annual Report 1991-92* at 11.

31 *Ibid.* at 12-13.

32 Kim Bolan shows that judges differ dramatically in their pronouncements about whether erasing audiotapes deprives an accused of *Charter* rights in criminal proceedings: *Loss of Faith: How the Air India Bombers Got Away with Murder*, *supra* note 21 at 359-60.

collecting intelligence or evidence. It also displays the limited ability of MOUs to smooth the edges of agencies with mandates that occasionally overlap. Finally, it shows that in the years immediately following its coming onto being, CSIS was staffed by people in job transition. Its organizational culture was hybrid, blending features that characterized a police organization, such as cracking a big case, with those that were also characteristic of an intelligence agency, such as the reluctance to share information. I will now discuss this topic in more detail.

1.2 Evolving professional cultures

I focus in this section on the evolution of the occupational and organizational culture of CSIS from its creation in 1984 to the present day, since the change in CSIS was much more pronounced than in the RCMP. I shall also briefly discuss the case of the RCMP and of the other Canadian police forces. By "occupational culture" I mean a set of beliefs, assumptions and values underpinning the *modus operandi* of the individual members of an agency (for example, whether they act alone or as a team). An agency's organizational culture consists of its mindset and the consequences of systemic features that are built into its structure (for example, whether it is centralized or decentralized). Needless to say, the organizational culture shapes the occupational culture. I use the words "professional culture" as shorthand to refer to both aspects of a work culture at the same time. It is important to stress that for me professional cultures translate into action in the field. I will distinguish the three different phases of CSIS's professional culture and I will present the cultural evolution of the RCMP as a whole.

1.2.1 *CSIS: From the primacy of field operations to the primacy of intelligence (1984-1991)*

After its creation in July 1984, CSIS first went through a difficult transitional phase during which **SIRC spearheaded its transformation**. When CSIS came into being, 95 per cent of the former personnel of the RCMP Security Service elected to transfer to the new agency and for several years, these former RCMP officers constituted more than 80 per cent of CSIS intelligence officers (IOs). As SIRC emphasized, "they brought the memories and habits of the RCMP with them."[33] CSIS also inherited all the files of the RCMP Security Service – 510,000 of them – many of which targeted individual and groups believed to be merely "subversive" and

33 SIRC *Annual Report 1986-87*.

presenting no clear and present threat to Canada. Human sources that had been recruited by the RCMP Security Service began to report to CSIS handlers and were a potential source of trouble.[34] The professional culture of CSIS was then marked by two features. I must emphasize that these were the predominant features of CSIS culture in the year that preceded the Air India bombings and during their aftermath.

First, the culture of CSIS was based on unwarranted suspicion rather than threat assessments rigorously grounded in fact. The RCMP's emphasis on counter-subversion, which was initially carried over to CSIS, testified to the pervasiveness of this culture of unwarranted suspicion.

Second, the approach taken by CSIS reflected the case-oriented approach of police work.[35] It was institutionally biased in favour of information gathering by **operational programs** – counter-intelligence and counter-terrorism – instead of advice to government.[36] Its Analysis and Production Branch stressed short-term tactical analysis and neglected basic strategic intelligence. It also favoured generalists who produced shallow analyses about many subjects over specialists who researched an issue in depth. This kind of approach was later the target of severe criticism by U.S. Senator Richard C. Shelby, who examined the FBI's intelligence failures in the months preceding the attacks against the United States on September 11, 2001. "Intelligence analysts," said Senator Shelby, "would doubtless make poor policemen, and it has become very clear that policemen make poor intelligence analysts."[37] Shelby summarized his diagnosis of this intelligence failure by denouncing the "tyranny of the case file." It was precisely this tyranny that was being exercised within CSIS. Even though they had been deprived of their peace officer powers, CSIS agents competed with RCMP investigators in trying to solve the bombing of Air India Flight 182. CSIS was on the case and would not let go.

CSIS closed the Sir William Stephenson Academy in 1987 because it believed that recruits with a police background needed no additional training and could make a "direct entry" into the Service. CSIS had apparently decided to hire only persons with a professional police background and had in

---

34 One of these sources – Marc-André Boivin – was recruited in 1973 by the RCMP Security Service and had risen to be an official in the Quebec labour movement. Mr. Boivin was facing bomb-related charges in 1988 when the media reported that he was a CSIS source, perhaps an *agent provocateur*: SIRC *Annual Report 1987-88* at 16-17.

35 SIRC *Annual Report 1986-87* at 13.

36 SIRC *Annual Report 1988-89* at 17.

37 U.S., Senate Select Committee on Intelligence, "September 11 and the Imperative of Reform in the U.S. Intelligence Community: Additional Views of Senator Richard C. Shelby, Vice Chairman, Senate Select Committee on Intelligence" (Washington, DC: Congress, 2002) at 62.

consequence no more need for a training academy, as former police officers were immediately integrated into the Service. This approach collided head-on with the policy of civilianization that had led to the creation of CSIS. SIRC declared that it was subsequently "stunned to hear that CSIS had hired 16 former police officers in the last quarter of 1986 and left no positions open for new recruits from the universities or civilian employment. As a result, the Academy has been closed down for a year, and further civilianization has been stalled."[38] In the opening words of its 1986-87 annual report, SIRC expressed its "mounting" concern that "civilianization [was] proceeding too slowly because of heavy recruitment of ex-police officers. This can only perpetuate the law-enforcement approach that Parliament intended to change when it adopted the *CSIS Act*."[39]

The Government reacted by creating the Independent Advisory Team on the Canadian Security Intelligence Service (IAT), led by the Hon. Gordon F. Osbaldeston.[40] The IAT tabled its report in October 1987. The report contained 34 major recommendations bearing on recruitment and training, the intelligence product, counter-subversion, the security intelligence network and various other matters. Following the publication of this report, the CSIS recruitment policy was revised and the Stephenson Academy was reopened. The Counter-Subversion Branch of CSIS was progressively disbanded and most of its files disposed of. The Analysis and Production Branch (APB) became the Requirements, Analysis and Production Branch (RAP) and was significantly expanded.

SIRC used the IAT report as its basis for promoting the transformation of CSIS into an *intelligence* agency with a role not merely to pile up facts, but to advise the government on the strength of thoughtful analysis. Its efforts met with success, and SIRC declared with obvious satisfaction, "The Cinderella story of the Analysis and Production Branch (RAP) continued in 1989-90. When we made a special study of RAP in 1987-88, we found it was a neglected step-sister in the CSIS family. Today it seems to be the glamorpuss. The change is good news."[41] For all practical purposes, CSIS had begun in earnest to change its law enforcement culture based on

---

38 SIRC *Annual Report 1986-87* at 44.

39 *Ibid.* at 1. "*CSIS Act*" is an informal abbreviation of the *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23.

40 Independent Advisory Team on the Canadian Security Intelligence Service, *People and Process in Transition* (report to the Solicitor General) (Ottawa: Ministry of Supply and Services Canada, 1987) [Osbaldeston IAT Report].

41 SIRC *Annual Report 1989-90* at 19 [footnotes omitted].

suspicion and caseload, and was developing an intelligence culture that used analysis to produce unbiased threat assessments for its various information consumers. Borrowing from Ericson and Haggerty,[42] CSIS agents had truly become "knowledge workers."

1.2.2 *CSIS: The end of the Cold War and the lean years – back to operations (1992-2002)*

The last decade of the 20th century would see the end of the Cold War and the crumbling of the Soviet Bloc. As the existence of national security agencies was in great part predicated on the muted conflict between the Western democracies and the Communist countries, the proclaimed end of this clash was bound to affect CSIS. CSIS began in 1992 to issue a public annual report that listed the types of its operations. This sudden public openness was a sign that CSIS was seeking alternative missions and was ready for new ventures. Indeed, from its peak of $244 million in 1993-95, the CSIS budget had plummeted to a low of $167 million in 1997-1998. SIRC's own budget was decreasing in the same proportion. The number of threat assessments produced by the Service declined from 843 in 1993-94 to 602 in 1995-96, and would continue to slide to 543 before the end of the century.

Although public safety – counter-terrorism – still accounted for 60 per cent of its activity, CSIS tried to resist its decline by becoming involved in new programs. Its 1997 public report thus mentions economic espionage, information warfare, nuclear proliferation and, most tellingly, transnational criminal activity. Some of these programs intruded on the operations of other agencies, most notably the RCMP in respect of transnational crime and the Communications Security Establishment (CSE) in respect of information warfare. However, the most significant development was the gradual phasing out of the former "glamorpuss" of CSIS, the RAP. In its 1996-97 secret report to the Government, the Director of CSIS did not mention RAP.[43] SIRC reviewed the intelligence production within CSIS and in its 1998-99 report noted that the Strategic Analysis Unit had been disbanded to allow the integration of strategic analysts into operations. More significantly perhaps, SIRC states that its review of the production of intelligence also identified "a troubling form of professional segregation within the Branch. RAP staff who are not classified as intelligence officers

---

42 Richard V. Ericson and Kevin T. Haggerty, *Policing the Risk Society* (Toronto: University of Toronto Press, 1997).

43 SIRC *Annual Report 1996-97* at 55.

(IOs) are treated differently in the areas of salary, training, and career advancement."[44] This statement was particularly meaningful because it closely paralleled a much earlier finding expressed in the 1981 report of the McDonald Commission.[45] The McDonald Commission report said that the most bitter members of the RCMP Security Service were the civilian analysts, who claimed to be victims of "administrative apartheid" within the Force.[46] From apartheid to segregation, it seemed that working conditions of the civilian analysts had not much improved in the 15 years that followed the McDonald Commission report. The renewed CSIS focus on operations was mirrored in the change in 1996-97 to SIRC's annual report, which now bore the title, *An Operational Audit of CSIS Activities.*

1.2.3 *CSIS: Rebirth – the war on terrorism*

On September 11, 2001 ("9/11"), two planes flew into the Twin Towers of the World Trade Center in New York. Another crashed into the Pentagon and a fourth crashed on its way to a Washington D.C. target after a rebellion by its passengers. These momentous events officially triggered the occupation of Afghanistan and of Iraq – actions which are said to be part of the larger war against terrorism declared by the United States.

CSIS's budget was increased by 30 per cent for fiscal year 2001-02. This increase was projected to grow annually to at least 36 per cent by fiscal year 2006-07. Things have evolved with so much haste since 9/11 that it is premature to ascertain what they mean for the professional cultures of CSIS and the RCMP. The 2007 preliminary hearing of the four teens accused of belonging to a terrorist organization in the alleged 2006 Toronto terrorist plot should shed some light on how this conspiracy was checked by the police. For the preliminary hearings of the four teens (out of seventeen accused) alone, there are apparently two million pages of evidence on three computer hard drives.[47]

I will limit myself to a few points.

A. *Ahmed Ressam.* Except for 9/11, the most important incident in respect of the U.S. war on terrorism occurred on December 14, 1999, when a U.S.

---

44 SIRC *Annual Report 1998-99* at 11-14, referring to SIRC Report #110 (Review of Intelligence Production).

45 Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security under the Law*, 2 vols. (Ottawa: Minister of Supply and Services Canada, 1981) ("McDonald Commission," Chair: David C. McDonald).

46 *Ibid.*, vol. 2 at 687.

47 M. Shepard, "Hearing into teens' role in terror case," *The Toronto Star* (January 15, 2007).

customs officer intercepted Ahmed Ressam, who used to live in Montreal, as he entered the U.S. with a rented car full of explosives. Ressam was planning to bomb the Los Angeles Airport on the advent of the new millennium. Although he was under CSIS surveillance, he left Canada to train in Afghanistan in 1998 and came back undetected in February 1999 carrying a passport under the name of Benni Antoine Norris. He prepared his terrorist plans unhampered by CSIS or any police force, and left for the United States, where he was arrested before accomplishing his attack. In its review of the Ressam affair, SIRC concluded that it saw "no evidence that it was a lack of vigilance on the part of the Service [CSIS] that contributed to Ressam's ability to escape detection after his return in 1999."[48] This assessment did nothing to dispel the belief in the U.S. that a culture of failure presides over the Canadian intelligence community and its partners in counter-terrorism. Although Ahmed Ressam was prevented from harming anyone in the United States, the impact on U.S. public opinion of his aborted attempt can be compared to the impact on the Canadian Indian community of the March 2005 acquittal of Malik and Bagri in the Air India trial. The Ressam fiasco may have driven Canadian counter-terrorist agencies to try to make up for this failure by becoming overly-aggressive. The Maher Arar affair lends some discomforting evidence in this respect.

B. *The counter-terrorism assemblage*. The lion's share of the 2002 counter-terrorism money was not awarded to CSIS but to CSE. Part of CSE's mandate is to protect Canada's communications and information structure. CSIS now harbours an Information Operations Centre IOC, which stores information resulting from CSIS investigations of threats to Canada's critical information infrastructure. The IOC may encroach upon CSE's mandate and generate a turf battle. In the same way, the Integrated Threat Assessment Centre (ITAC) was created in July 2004 to transmit threat assessments quickly to decision makers. ITAC is a cooperative initiative where 11 Canadian agencies involved in counter-terrorism at the national, provincial or municipal level are assembled. Among its ITAC partners, CSIS is supposed to be the first among equals.[49] The current director of ITAC was appointed in July 2005 and is seconded from the RCMP. SIRC found the level of co-operation between CSIS and other

---

48 SIRC *Annual Report 2002-03* at 6, 71.
49 SIRC *Annual Report 2005-06* at 9.

domestic agencies to be both appropriate and productive.[50] However, as noted before, SIRC has a tendency to downplay the frictions between agencies.

Making a splash in the war against terrorism is a big prize nowadays, as I found in the course of my research in policing in Quebec. Before 9/11, counter-terrorism intelligence was a responsibility of the *security* intelligence unit of the *Sûreté du Québec* (SQ, the Quebec provincial police). However, as soon as the counter-terrorism stakes were increased by 9/11, responsibility for collecting this kind of intelligence was transferred to the *criminal* intelligence unit of the SQ, with the strong backing of the Criminal Investigation Department (CID). Similarly, it is far from a foregone conclusion that the present counter-terrorism assemblage will perform as an integrated whole and that CSIS will succeed in asserting its leadership as the first among equals.

One final development within CSIS is difficult to assess because it is taking place informally. CSIS is a domestic intelligence agency, like its British counterpart, the Security Service (MI5[51]), and the Australian Security Intelligence Organisation (ASIO). A reading of CSIS and SIRC annual reports leaves no doubt that CSIS is becoming more deeply involved in collecting foreign intelligence and is increasing its number of Security Liaison Officers (SLOs). As long as there will be no formal recognition (for example, through legislation) of this unheralded push into foreign intelligence, we will not be able to measure its influence on the professional culture of CSIS.

1.2.4 *The RCMP's evolution*

As I previously said, it is not so much the professional culture of the uniformed RCMP that is at stake as its attendant impact on its plainclothes investigators. The main focus in the RCMP from the 1980s to date lay in spearheading the community policing movement in Canada.[52] The meaning of community policing is disputed. Whatever it may be, it rests on police visibility and involves almost exclusively uniformed patrol

---

50 SIRC *Annual Report 2001-02* at 12.

51 "MI5" (Military Intelligence section 5) was the name given to Britain's security service in 1916. MI5 was subsequently renamed the "Defence Security Service" (in 1929) and the "Security Service" (in 1931), the name it retains today. However, the Service is still often simply called MI5: http://www.mi5.gov.uk/output/Page65.html.

52 A. Normandeau and B. Leighton, *A Vision of the Future of Policing in Canada: Police-Challenge 2000: Background Document* (Ottawa: Police and Security Branch, Ministry of the Solicitor General, 1990).

persons deployed in the field. There is a consensus among researchers that this movement widened the gap between patrol persons in uniform and plainclothes investigators. To that extent, the early embracing of community policing by the RCMP may not have enhanced the quality of its investigative performance in 1985.

Community policing evolved into problem-oriented policing, which implied the collection of data on community problems and their analysis according to the SARA method – Scanning, Analysis, Response and Assessment. Problem-oriented policing was only a step away from intelligence-led policing (ILP), which is increasingly the new police paradigm. However, the RCMP appeared to resist this paradigm. In a 2005 public talk, Giuliano Zaccardelli, then RCMP Commissioner, remarked that ILP "reeks of secret service, spy agency work – the capital "I" in "Intelligence."[53] It should be mentioned that a federal commission of inquiry – the O'Connor inquiry – was at that time investigating the RCMP and the Commissioner for sharing with U.S. agencies] unverified intelligence on the alleged involvement of Canadian citizen Maher Arar and others in terrorism.[54] This may explain in part why Commissioner Zaccardelli distanced himself from ILP. It is also possible that he was expressing the traditional police bias favouring action over information.

As the Thacker Committee[55] noted, the RCMP always kept a stake in national security through its National Security Investigations Directorate (NSID) and National Security Investigations Sections (NSIS), and still took aggressive action against its targets. After 9/11, the RCMP boosted its involvement in national security and played the lead role in the 2006 arrest in Toronto of 17 persons allegedly involved in a bomb plot. In so doing, it apparently performed a "sting operation" whereby the suspects allegedly tried to buy three tonnes of ammonium nitrate from an RCMP infiltrator.[56]

There is an important conclusion to be drawn from the previous analyses: **Security intelligence agencies such as CSIS are much more susceptible to the volatile global political environment than are law**

---

53 Giuliano Zaccardelli, Speaking notes for a presentation on intelligence-led policing at the Canadian Association of Chiefs of Police Conference, Ottawa, Ontario, August 23, 2005.

54 Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar*, vol. 3 (Ottawa: Minister of Public Works and Government Services, 2006) (Chair: Dennis O'Connor).

55 Canada, House of Commons, *In Flux but not in Crisis: Report of the Special Committee on the Review of the CSIS Act and the Security Offences Act* (Ottawa: Supply and Services Canada, 1990) at 103, 187 [Thacker Committee Report].

56 J. Goddard, "Fertilizer usually sold just to farmers," *The Toronto Star* (June 7, 2006) A6.

enforcement agencies. Although crime varies, it will never disappear, and law enforcement forces will always be needed. In contrast, there was a time when security intelligence agencies may have believed that they were out of a mandate, and as a result made the necessary moves to survive. This sensitivity to the global political context is a crucial difference between police and national security agencies.

2. MAJOR CONTRASTS BETWEEN SECURITY INTELLIGENCE AND POLICE ORGANIZATIONS

I will follow a dual methodological approach in pursuing my discussion of the differences between the professional culture of law enforcement and security intelligence agencies. First, I discuss major and minor contrasts in culture through incidents that illustrate these contrasts. Second, I will offer a theoretical synthesis of the differences. The major sources of contrast that I want to examine are (1) competition; (2) mandates, from which stem the divergent needs of collecting security *intelligence* and of gathering *evidence* to support court proceedings; (3) the related issue of infiltration using human sources; (4) information analysis; and (5) the fight against transnational crimes.

2.1 Competition

There is an undeniable difference between police forces and security intelligence agencies. The members of police forces have special powers of coercion stemming from their legal status as peace officers, and they are responsible for enforcing the law. Members of civilian intelligence agencies have no such powers. However, since security intelligence organizations are responsible for protecting national security and are also involved in protecting citizens against terrorist violence, they can be said to be *policing* agencies, although they are not police in the legal and institutional sense. The literature on policing culture generally agrees that such a culture rests on an entrenched dichotomy between the "in-group" and the "out-group."[57] The McDonald Commission report went as far as comparing the RCMP to a "religious Order."[58] The flip side of this dichotomy is *competition*. Policing agencies behave aggressively towards out-groups, including other policing agencies. Consequently,

57 Janet Foster, "Police cultures" in Tim Newburn, ed., *Handbook of Policing* (Cullompton (Devon; UK), 2003) at 197; P.A.J. Waddington, "Police (canteen) sub-culture: an appreciation" in Tim Newburn, ed., *Policing: Key Readings* (Cullompton (Devon, UK): Willan Publishing, 2005) 364 at 379.

58 Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security under the Law*, vol 2. (Ottawa: Minister of Supply and Services Canada, 1981) ("McDonald Commission," Chair: David C. McDonald) at 689.

the competition between CSIS, the RCMP and other law enforcement agencies is not in my view merely a derivative effect that can be explained by something else (for example, different mandates). It is a core feature embedded in the professional culture of policing agencies and one that generates its own effects. In brief, CSIS and the RCMP only needed to be policing agencies in their own right to compete against each other.

In one of its early annual reports, SIRC observed that the term "healthy tension" was used to describe the relationship between CSIS and the RCMP, adding that it would even be healthier if it were less tense.[59] For instance, SIRC was "puzzled and disappointed" that it took six years to resolve the issue of access by CSIS to the Canadian Police Information Centre (CPIC), a database managed by the RCMP.[60] CSIS was granted partial access to CPIC only in 1990. Without taking into account any in-bred competition between policing agencies, the RCMP reluctance was indeed surprising. After all, CSIS was at the time essentially staffed with former colleagues. However, **the working relationship of CSIS with the RCMP is not only about facts but also about perceptions.** For instance, CSIS and the RCMP successfully concluded one counter-terrorism investigation that involved an "important friendly country." Despite the ultimate success of the operation, SIRC was concerned that "the possible damage would lie in the insecurity felt in an important friendly country about the ability of CSIS and the RCMP to work together."[61]

SIRC assessed the cooperation of CSIS with the RCMP in an inquiry conducted over two years (1997-1999). It concluded that the relationship could be characterized as one of "genuine and fruitful cooperation," with two exceptions: RCMP use of CSIS intelligence in criminal proceedings and CSIS responsibility in the area of transnational crime.[62] However, SIRC added an important reservation to this overall assessment by declaring that "incidents that came to our attention which in part gave rise to our study of the CSIS-RCMP relationship indicate that there *may be less to be sanguine about at the regional level*."[63] There are many instances of those regional difficulties. An MOU between CSIS and the SQ and

---

59 SIRC *Annual Report 1986-87* at 27.
60 SIRC *Annual Report 1988-89* at 16.
61 SIRC *Annual Report 1989-90* at 38.
62 SIRC *Annual Report 1998-99* at 24.
63 SIRC *Annual Report 1997-98* at 30, referring to SIRC Report #101 (CSIS Cooperation with the Royal Canadian Mounted Police – Part I) [emphasis added].

Quebec municipal forces was signed only in 1992, eight years after the creation of CSIS. In one unidentified region, the relations of CSIS with a law enforcement agency were so tense that in one case the police used subpoena powers to compel the attendance of CSIS officers as witnesses at a trial. In another case, the same law enforcement agency **alleged criminal wrongdoing on the part of CSIS** to get a search warrant to obtain a CSIS document from a third federal government agency.[64]

Although it has regional offices and liaison officers, CSIS is highly centralized, whereas the RCMP's operational structure is decentralized and dispersed among the provinces. In all provinces except Ontario and Quebec, an RCMP division enters into an agreement with the provincial government and operates with a margin of independence from RCMP headquarters. Problems that may be ironed out at the headquarters level through MOUs keep arising at the regional level, either with an RCMP detachment or a local law enforcement agency. We must recall that the Air India investigation was in great part conducted at the local level in British Columbia.

2.2 Preventive intelligence versus prosecutorial evidence

We previously saw that there were two areas of concern about collaboration between CSIS and the RCMP: the disclosure of CSIS intelligence in public criminal court proceedings and the self-attributed responsibilities of CSIS in the area of transnational crime. I will now address the first of these concerns. Briefly stated, the mandate of CSIS is to collect and disseminate information about threats to the security of Canada, using sources and investigative methods which must be protected in the interests of national security. The RCMP's mandate is to perform the attendant police functions – including mustering incriminating evidence – in relation to those threats. This framing of the respective responsibilities goes back to the Mackenzie Commission.[65] The Mackenzie Commission report emphasized the clear difference between the police and the security intelligence mandates.[66] This emphasis was carried over to the McDonald Commission and has never been questioned to this day.

These two mandates are complementary, as the September 2006 MOU stated, but in reality they result in clashes over the issue of public

---

64 *Ibid.*, referring to SIRC Report #103 (A Problematic Case of Inter-agency Cooperation) at 32-34.

65 Canada, Royal Commission on Security, *Abridged Report of the Royal Commission on Security* (Ottawa: Queen's Printer, 1969) (the "Mackenzie Commission") at para 55.

66 *Ibid.* at para. 57.

disclosure by the police – by the Crown – of the sources, methods and covert intelligence of CSIS to secure a conviction. This source of tension has been described as "unavoidable."[67] Since 1969, not one government body that examined the relations between CSIS and the RCMP, including the current Air India Inquiry (in its terms of reference),[68] has failed to refer explicitly to sources of tension. The tension became more acute after the Supreme Court of Canada's *Stinchcombe*[69] ruling on disclosure of Crown evidence to the defence. There are opinions to the effect that these disclosure obligations have become intractable problems. For example, in its *Annual Report 1998-99*, SIRC argued that, "[t]here is no obvious solution to this conundrum within the existing Memorandum of Understanding or under existing legislation. While the potential impact of changing the law is open to debate, what is not in doubt in our opinion is the potential for damage to national security operations should the situation be left unchanged."[70]

Issues surrounding the public disclosure of CSIS intelligence can be separated into at least four distinct categories: (1) the disclosure of CSIS files; (2) the transmission to law enforcement agencies of original material (letters, documents, audiotapes, videotapes, etc.); (3) the public testimony in court of CSIS operatives; (4) the disclosure of the identity of CSIS sources and testimony in public. The last issue is the most problematic.[71] According to my own experience as director of research of a commission of inquiry that addressed the issue of security service informants (the Keable Commission),[72] the circumstances in which an informant is heard and the measures to protect an informant's identity in court proceedings make no difference. The informant (also known as a 'human source' in police parlance) will immediately be identified by any defence lawyer worth his mettle as soon as he or she comes forward.

---

67 SIRC *Annual Report 1989-90* at 16; *Annual Report 1989-99* at 41.

68 In addition to the Mackenzie and McDonald Commissions, several other bodies addressed this issue: the Special Committee of the Senate on the Canadian Security Intelligence Service and its report, *A Delicate Balance: A Security Intelligence Service in a Democratic Society*, *supra* note 10; Independent Advisory Team on the Canadian Security Intelligence Service, *People and Process in Transition*, *supra* note 40 at 5; *In Flux but not in Crisis: Report of the Special Committee on the Review of the CSIS Act and the Security Offences Act*, *supra* note 55 at 15; SIRC *Annual Report 1987-88* at 32; *Annual Report 1989-90* at 5; and, more generally, SIRC *Annual Report 1997-98* and *Annual Report 1998-99*.

69 *R. v. Stinchcombe*, [1991] 3 S.C.R. 326.

70 SIRC *Annual Report 1998-99* at 22.

71 *Ibid.* at 21.

72 Québec, *Rapport de la Commission sur des Opérations Policières en Territoire Québecois* [*Keable Report*], (Québec: Ministère des Communications, 1981).

In order to show what is at issue in the disclosure of an informant's identity, I will review the legal proceedings in the case of Santokh Singh Khela and Kashmir Singh Dhillon.

1. **1986:** Santokh Khela and Kashmir Dhillon, members of Montreal Babbar Khalsa (an extremist Sikh organization), were convicted of plotting to bomb an Air India jet in New York. The Crown's case rested on the testimony of an informant claiming to have been paid $8,000 to blow up a jet. This informant – "Billy Joe" – was originally handled by the Quebec Provincial Police (QPP), who were co-operating with the RCMP and the FBI on this case. According to the QPP and RCMP handlers of Billy Joe, the accused wanted to blow up a plane in New York. They were "stung" by being put in contact with an FBI agent who posed as a bomb expert ready to contract to blow up a plane. The FBI agent eventually got them arrested. The accused said that the money was paid to Billy Joe to procure a stolen car (It was also claimed that it was paid for Billy Joe to kill an Indian journalist by the name of Hayer.).[73] Crucially, Billy Joe never testified in the 1986 proceedings.

2. **First appeal.** Khela and Dhillon appealed their convictions to the Quebec Court of Appeal. On December 9, 1991, their appeal was granted on the ground that "the trial judge erred in law in twice refusing to order the witness known as Billy Joe to be produced to testify at the trial."[74] A new trial was ordered.

3. **Second trial.** A second trial was held in 1992. The charges were stayed by Steinberg J. of the Quebec Superior Court because the Crown failed to meet the disclosure requirements formulated by the Quebec Court of Appeal in 1991. In addition, the informant's testimony did not satisfy the *Stinchcombe* disclosure requirements: Billy Joe testified outside the courtroom wearing a hood; the interview could not be taped and there was no court reporter; even the identity of the person wearing the hood was put in doubt by the defence. Both accused were freed after serving nearly six years in prison.

---

73 Bolan, *Loss of Faith: How the Air India Bombers Got Away with Murder*, *supra* note 21 at 147.
74 *R. v. Khela* (1991), 68 C.C.C. (3d) 81.

4. **Second appeal (to the Quebec Court of Appeal).** The Crown appealed Steinberg J.'s stay of proceedings to the Quebec Court of Appeal. The Court of Appeal ruled against the decision to stay the proceedings.[75]

5. **Third appeal (to the Supreme Court of Canada).** The defence appealed the Quebec Court of Appeal ruling to the Supreme Court of Canada. On November 16, 1995, the Supreme Court ruled that "the Crown totally failed to make full disclosure *prior to trial* in relation to Billy Joe" as required by the Court of Appeal in deciding the appeal of 1991, and that the Crown was in breach of section 7 of the *Charter*. The Supreme Court concluded that the terms of disclosure set by the Quebec Court of Appeal in its 1991 decision "accord with the decision in *Stinchcombe*."[76] The Supreme Court ordered another new trial.

6. **Third trial.** On the basis of a very muddled situation in respect of the non-disclosure of police notes relating to their informant Billy Joe the defence once more presented a claim for a stay of proceedings. Martin J., the trial judge, ordered a permanent stay of proceedings in what the Quebec Court of Appeal later called "a very detailed and articulate judgment."[77]

7. **Fourth appeal (to Quebec Court of Appeal).** The 1996 decision of Martin J. was appealed to the Quebec Court of Appeal, which ruled for a third time in this case. Proulx J.A. dismissed the appeal using unusually strong language: "This case, in my opinion, has reached a stage where, as Martin J. concluded, the serious prejudice resulting from the failure to disclose is not "remediable", using here the approach taken by the Supreme Court (R. v. O'Connor, supra). To put it bluntly, "enough is enough."[78]

This discussion shows first of all that the stakes in the intelligence versus evidence issue are quite high. Criminal proceedings that use evidence given by an informant against alleged terrorists can be unremitting, with massive economic and social costs for all parties. The proceedings in this case lasted for more than twelve years. Taking into account the costs of

---

75 *R. v. Khela* (1994), 92 C.C.C. (3d) 81.
76 *R. v. Khela*, [1995] 4 S.C.R. 201 at 203.
77 Unreported judgment 9 August, 1996.
78 *R. v. Khela*, (1998) 126 C.C.C. (3d) 341).

the police investigation, the police involvement in the preparation of the case, the testimony of the police witnesses and the informant, and the court proceedings in three trials and four appeals at all levels of the criminal justice system, including the Supreme Court of Canada, the whole process cost huge amounts of taxpayer money, to little avail. All parties implicated actually lost. The defendants spent six years in jail before their acquittal. The police and the Crown did not get the convictions they were seeking. The case also demonstrated that the *Stinchcombe* ruling placed the confidentiality of the identity of informants in jeopardy, increasing the gap between law enforcement organizations and agencies dedicated to the collection of intelligence.

2.3 Infiltration by human sources

SIRC began its special 1994 report[79] on the infiltration of the Heritage Front by a human source in the pay of CSIS with a C.S. Lewis quote: "Dream furniture is the only kind on which you never stub your toes or bang your knee." The handling of human sources is the field of policing where the difference between dream and real informants is the greatest.[80] I will limit my discussion of the complex and unruly topic to five points. Although undercover police and security intelligence agents play an important role, I will make my points exclusively about informants who are not regular members of policing agencies. This is because I consider discussing these informants is more relevant for this Commission's mandate than is discussing the work of undercover police.

A. *The various uses of informants*: The infiltration of organizations by informants (human sources) is the most intrusive of investigative techniques. Whether they answer to police or to intelligence agents, paid human sources have one thing in common: they enjoy a covert and limited licence to commit crimes to penetrate deeper into a criminal or terrorist organization and to protect their cover.[81] SIRC drew a crucial distinction between "passive" and (criminally) "active" sources, and further argued that "if CSIS were to use only "passive" sources . . . the quality of the information available to the intelligence community and to police

---

79 Security Intelligence Review Committee, *The Heritage Front Affair*, *supra* note 11.

80 Jean-Paul Brodeur, "Undercover Policing in Canada: A Study of its Consequences" in C. Fijnaut and G.T. Marx, eds., *Police Surveillance in Comparative Perspective* (The Hague: Kluwer Law International, 1995).

81 *Ibid.* at 89; Peter Reuter *Disorganized Crime: The Economics of the Visible Hand* (Cambridge: MIT Press, 1983); Jean-Paul Brodeur "Undercover Policing in Canada: A Study of its Consequences" in C. Fijnaut and G.T. Marx, eds. *Police Surveillance in Comparative Perspective* (The Hague: Kluwer Law International, 1995) at 89.

forces would be considerably less useful at best or useless at worst. *Most good sources are active.*"[82] Because of their "activity," human sources are unavoidably suspected of entrapping their targets when they are acting on behalf of the police, or of being *agents provocateurs* if employed by a intelligence security agency. The police usually make short-term use of their informants, perform sting operations[83] with their assistance, and have no qualms about calling informants to testify in court, since governments have witness protection programs. Security intelligence agencies such as CSIS infrequently mount sting operations, since they have no law enforcement mandate; they try to use sources for as long as possible and go to great lengths to protect their identity.

B. *Human sources and the courts*: Because of their involvement in criminal activities and their police or security intelligence stipend, human sources have over the years lost a significant amount of credibility in court. It is now difficult to secure a conviction based solely on the testimony of an informant. This distrust extends to witnesses who were linked through some form of "activity" (for example, an amorous liaison) to a person being prosecuted.

C. *Cultures of containment and of interruption*: I have already quoted SIRC's 1994 pronouncement that most good sources had to be active. Much earlier, SIRC had addressed the problem of intelligence agencies closing their eyes to a lesser crime in order to keep them open to potentially bigger crimes. SIRC first stated its agreement with the view of the McDonald Commission that a security intelligence agency had a duty to tell the police what it knew about criminal activities. However, SIRC also acknowledged exceptions to this rule "when a police investigation, and perhaps evidence at a subsequent trial, would irremediably compromise a vital security operation."[84] This takes us to the heart of the professional culture of a security service, whether police or civilian, as it was described by the Québec Keable Commission, of which I was director of research.[85]

---

82 Security Intelligence Review Committee, *The Heritage Front Affair*, *supra* note 11 at section 13.11 [emphasis added].

83 A sting operation uses informants and also undercover agents to facilitate the perpetration of a crime in a context designed to record evidence for the prosecution. Classic examples involve police informants or police undercover agents posing as drug buyers and then arresting the sellers *in flagrante delicto*. The 1986 case involving Khela and Dhillon was an unusual operation involving a source ("Billy Joe") and a FBI undercover agent (Frank Miele) posing as an explosives expert ready to bomb a plane for Khela and Dhillon. If the 17 persons arrested in 2006 for an alleged Toronto terrorist plot did buy ammonium nitrate from an RCMP source, as claimed by the media, this would make the police operation at least in part a sting operation.

84 SIRC *Annual Report 1986-87* at 26.

85 See also Jean-Paul Brodeur, "Legitimizing Police Deviance" in Clifford Shearing, ed., *Organizational Police Deviance* (Toronto: Butterworths, 1981) at 127.

Between November 1970 and 1973, the counter-terrorist unit of the Montreal police transformed the *Front de Libération du Québec* (FLQ) into a police colony by riddling it with police informants. The counter-terrorism unit limited its actions to monitoring lesser crimes (for example, fire-bombing) while using its informants to steer the group in a direction where it eventually stopped being a real threat. More than twenty years later, SIRC rediscovered this security service culture of containment: "We are also cognizant of the danger that in destroying one group, as opposed to watching it, another one which is worse may be created."[86] In contrast, the police build unrelated individual cases to interrupt criminal activities. Such interruptions are sometimes long-lasting and even final. In many cases, the interruption of criminal activity is only temporary.

D. *Means over ends.* Throughout his work the great police reformer Herman Goldstein criticized what he called the "means over ends syndrome." Agencies suffering from this syndrome give priority to "means" that are germane to achieving organizational ends – for instance, crackdowns on small-time drug-traffickers that boost the police statistics, but have no effect on the drug trade itself – over its external "ends" of providing an efficient service to society (for example, protection from harm). There is a risk that the use of long-term infiltration may fall prey to the means over ends syndrome. Take the case of the CSIS officer who claimed in *The Globe and Mail* to have destroyed audiotapes that may have been helpful to the Air India investigation in order to protect the identity of his informants Assuming that the CSIS officer was being truthful, his loyalty to his informants was in a way laudable. However, the bombing of Air India Flight 182 and the explosion at Narita Airport resulted in 331 casualties and was one of the worst terrorist attacks to have occurred worldwide – certainly the worst in Canadian history. In those circumstances, giving priority to the protection of one's informants over solving this monstrous crime is tantamount to losing sight of the point that infiltration is a means towards the end of protecting the nation and its people. Infiltration and the protection of informants is not an end for its own sake. **In my view, there needs to be a clear policy to cure intelligence agencies of the means over ends syndrome in the practice of infiltration and in the handling of informants.** The long-term containment argument is not valid in all circumstances, and neither is the need to protect informants from retaliation, including death. If law enforcement agencies succeed in protecting informants who testify in public criminal proceedings through

---

86 SIRC, *The Heritage Front Affair*, *supra* note 11 at section 13.11.

witness protection programs, I don't see why security intelligence agencies could not.[87]

E. *Informant asymmetry*. It cannot be assumed that an informant answers to only one handler or is active in only one criminal field. In my research on informants for the Quebec Keable Commission, I came across informants who were "feeding" two or more "handlers" or "control officers" at the same time. These handlers belong to different police forces, and some informants were expert at pitting their handlers against each other for the informant's own benefit. In other cases, a person may have been very good at compartmentalization – for example, being a drug informant while at the same time pursuing terrorist activities. Such an informant might even enjoy the protection of his narcotics handler from potentially being arrests by the counterterrorism unit. Research into such issues **is impossible to pursue from open sources. Only the Commission can follow up on these issues.**

2.4 Analysis of information

In the parlance of the intelligence community, intelligence is a product that is obtained by applying techniques of analysis to covert or open source information. I attempted to show in section 1.2.1 of this paper that the former members of the RCMP Security Service who staffed CSIS in its first years were still imbued with a police culture that gave priority to operations over threat assessment and that also gave priority to short-term tactical tips over long-term strategic intelligence. In addition to SIRC's efforts, it took the recommendations of Osbaldeston's IAT to turn things around. I also referred to U.S. Senator Richard C. Shelby's views on the failure to prevent 9/11, views which despaired of the FBI's ability to produce security intelligence and which led to a proposal to replace the FBI with another agency patterned on the British MI5.

The RCMP and CSIS embarked on a common intelligence venture in March 1996. News of the venture was leaked to the media in 1999. This project, called "Sidewinder," was to measure the extent of China's economic espionage and assess the harm inflicted on Canadian society

---

87 The British actually succeeded in protecting their supergrasses' informants who testified against indicted IRA terrorists in criminal proceedings. See Tony Gifford, *supergrasses: the use of accomplice evidence in Northern Ireland* (London: Cobden Trust, 1984); Amnesty International, *United Kingdom – Northern Ireland: killings by security forces and "supergrass" trials* (London (UK): Amnesty International, 1988); Steven Greer, *Supergrasses: A Study in Anti-Terrorist Law Enforcement in Northern Ireland* (Oxford: Oxford University Press, 1995).

by Chinese criminal gangs ("Triads"). The project was modest at the beginning, involving two analysts from the RCMP and two from CSIS. However, the project generated a feud that embroiled high-ranking officers of both agencies. Although the project started in March 1996, it was apparently in limbo until the RCMP analysts issued a first draft of the report in June 1997. CSIS reviewed this first draft, and the Director General of RAP (Requirements, Analysis & Production Branch) concluded that the report's findings were "based on innuendo, and unsupported by facts."[88] The RCMP/CSIS team resumed work and the conflict escalated. In May 1998, it was the RCMP's turn to complain about a number of factual errors in the CSIS revised draft. In December 1998, the Deputy Director General of RAP wrote to the RCMP Officer in Charge, again pointing to innuendo in the then-current draft report and saying that CSIS did not concur with the inclusion of such items in the report. She wrote, "We do not have factual evidence of our suspicions and the Service is uncomfortable with the obvious challenges that could be raised by the readership."[89] Despite these travails, both agencies finally agreed to approve a final version of the Sidewinder report in January 1999. SIRC studied the first RCMP draft of the report and found it to be "deeply flawed and unpersuasive . . . . Whole sections employ leaps of logic and non-sequiturs to the point of incoherence; the paper is rich with the language of scare-mongering and conspiracy theory. Exemplifying the report's general lack of rigour are gross syntactical, grammatical and spelling errors too numerous to count."[90] SIRC commended the Service for implementing standards of the highest possible quality in producing threat assessments. In customary euphemistic fashion, it concluded that Project Sidewinder had inflicted no lasting damage to the broader CSIS-RCMP working relationship. Indeed, considered in isolation, none of the incidents reviewed by SIRC was ever serious enough to reverberate throughout both agencies and pit them against each other. However, it is an open question whether the sum of these incidents undermined that working relationship.

It should be asked whether SIRC's severe judgment on the work of RCMP analysts was biased in favour of CSIS Upon reading the O'Connor reports about the Maher Arar affair, I am persuaded not only that SIRC was not biased against the RCMP, but that the RCMP should have taken stock of SIRC's assessment. The O'Connor reports fault the RCMP for sharing with its U.S. partners information about Maher Arar that was both inaccurate

---

88 SIRC *Annual Report 1999-2000* at 5, referring to SIRC's Report #125 (at 3-9), its analysis of RCMP-CSIS relations during Project Sidewinder.

89 SIRC Report #125, *ibid.* at 6.

90 *Ibid.*

and incendiary.[91] On the other hand, the O'Connor report commended CSIS for the caution and precision of its threat assessment.[92]

2.5 Transnational crime

The involvement of CSIS in the fight against transnational crime seems to have been a transitory investment of the Service. It was not part of CSIS operations during the Cold War and does not seem to be part of its priorities after 9/11. I will briefly discuss the issue because it is mentioned by SIRC as one of the two areas of friction with the RCMP, the other being the intelligence versus evidence conundrum discussed above.

Apart from RAP, security clearances and immigration screening activities, CSIS performs the following operations: targeting, special investigations , surveillance (physical and electronic), getting warrants and acting upon them, community interviews, and sensitive investigations .[93] Most of these activities share common features with police investigations and have the potential to encroach upon police responsibilities. In 1993, there was some concern in government that certain aspects of transnational organized crime were threatening the social fabric and economic security of Canada. Since protecting Canada's national security was at the core of the mandate of CSIS, the Service followed up on this governmental concern and set up a Transnational Criminal Activities Unit within its CI (Counter-Intelligence) Branch in 1995, thus distinguishing transnational criminal activity from transnational terrorist threats.[94] This was perceived by SIRC as "a significant departure from the Service's traditional area of responsibility."[95] This move by CSIS was in line with the re-orientation of security intelligence throughout the Western world, with most agencies seeking a new *raison d'être* after the end of the Cold War.[96]

CSIS claimed that its involvement in this domain was limited to collecting strategic intelligence, and that it left tactical law enforcement activities to the police. The police felt that the abstract distinction between strategy and tactics did not provide a clear standard to separate police and

---

91 *Report of the Events Relating to Maher Arar*, *supra* note 54 at vol. III, chapter I, section 5.1.5.3. See also vol. III, chapter III, section 2.4.

92 *Ibid.* at vol. III, chapter III, section 7.6.

93 Sensitive investigations are investigations of persons who are members of a sensitive institution: SIRC *Annual Report 1997-98*, referring to SIRC Report #97 (Annual Audit of CSIS Activities in a Region of Canada) SIRC, 1997-98: report 97).

94 SIRC *Annual Report 1995-96* at 15.

95 SIRC *Annual Report 1998-99* at 5.

96 Jean-Paul Brodeur "Cops and spooks: the Uneasy Partnership" in Tim Newburn ed. *Policing: Key Readings* (Cullompton (Devon) Willan Publishing, 2005)

security intelligence responsibilities. It was also obvious that CSIS agents did not have the training and knowledge to operate in a field as complex as money-laundering, where the RCMP had scored notable victories (for example, by operating a fake money-changing office in Montreal where the RCMP monitored criminals laundering money). In addition to these two problems, the familiar regional quarrels over the denial of access to CSIS intelligence to local police agencies began to flare. SIRC concluded its assessment of the incursion by CSIS into the field of transnational crime in an unusually critical tone, suggesting that the Service "may not be equipped either by tradition or by training to take on the task."[97] **The upshot of this discussion is that the friction between CSIS and the police establishment is a two-way street. The first problem lies in denying access to one's turf and files to another party (defence); the reverse problem lies in aggressively asserting one's stake in the other party's traditional responsibilities (offence).**

3. MINOR CONTRASTS BETWEEN SECURITY INTELLIGENCE AND POLICE ORGANIZATIONS

The word "minor" here does not mean that the contrasts discussed are of lesser importance. However, they have a more limited scope. I shall address the issues of (1) recruitment; (2) training; (3) internationalization; (4) human rights; and (5) accountability. First, however, I address the question of ethnocentricity, a common trait of all police and security intelligence organizations.

3.1 Ethnocentricity

Ethnocentricity is a strong feature of all policing organizations. They have been criticized repeatedly for practicing racial and ethnic discrimination. Police sociologists such as Egon Bittner and Robert Reiner have stressed that one of the original features of the unofficial police mandate is the policing of immigrants and foreigners. On a less dramatic level, policing organizations such as the RCMP have had difficulty respecting Canada's linguistic duality and implementing policies that promoted the rights of their French-speaking minority members. When CSIS came into being in 1984, it was staffed by ex-members of the RCMP Security Service. The situation with bilingualism and relations with its French-speaking

---

97 SIRC *Annual Report 1998-99* at 10.

members was so tense that it spurred SIRC to table a special report to remedy the situation.[98]

Notwithstanding the perennial Canadian issue of bilingualism, ethnocentricity is a grievous impediment in the struggle against terrorism for several reasons:

(1) CSIS had no translator who could render in English the conversations of Sikh suspects intercepted through wiretaps, causing delays of as much as six weeks in obtaining access to this information at the beginning of the Air India investigation.[99] The dearth of competent translators in the U.S. intelligence community has been lamented in all reports that examined the 9/11 tragedy;

(2) The almost total absence of members from ethnic minorities in CSIS or RCMP national security units makes it almost impossible to perform undercover work and to infiltrate home-grown terrorist networks;

(3) The less that policing agencies try to be representative in their recruitment policies of the general makeup of the Canadian population, the greater their vulnerability becomes to accusations of external ethnic profiling;[100]

(4) The screening of immigrants, traditionally a low-prestige occupation at CSIS,[101] is now a task of crucial importance that cannot be adequately performed by an ethnocentric agency.

---

98 Security Intelligence Review Committee, *Closing the Gaps: Official Languages and Staff Relations in the Canadian Security Intelligence Service* (Ottawa: Minister of Supply and Services Canada, 1987).

99 Bolan, *Loss of Faith: How the Air India Bombers Got Away with Murder*, *supra* note 21 at 72-73. (Bolan, 2005: 72-73).

100 "According to Aly Hindy of the Salaheddin Islamic Centre, Mr. Ahmad blamed constant spying by CSIS for forcing him into criminal activity:" Colin Freeze, "How the police watched the plan unfold," *The Globe and Mail* (June 7, 2006) A8 Even if they sound spurious to the majority of Canadians, such accusations about spying find an audience among ethnic minorities.

101 One of the targets of the so-called 'Toronto bomb plotters' was allegedly the Toronto office of CSIS. Having given a course on terrorism at the CSIS academy, I was invited to the graduation ceremony of the new recruits. It was announced at this graduation celebration to which CSIS unit a recruit was appointed. The frustration of the new officers appointed to immigration screening was quite obvious (CT and CI were the prized appointment).

3.2 Recruitment

When it came into being in July 1984, CSIS was first staffed with former members of the RCMP Security Service, 95 per cent of whom had opted to join the new agency. They brought with them a *hybrid* culture. Part of this culture was the RCMP culture of a para-military police force. They also brought with them something specific to the RCMP Security Service, which the McDonald Commission described as "institutionalized wrongdoing."[102] The initial recruitment problem was not that CSIS was staffed in this way – there was no other option than to admit the former members of the RCMP Security Service – but that its recruitment policy **kept on** favouring recruits with a police background, recruits who were then directly integrated into CSIS without the benefit of additional training.

Following SIRC's energetic action and the Osbaldeston IAT Report, CSIS embarked on a recruitment campaign in 1989 and received 8,447 applications, 1,116 of which were judged to have high potential.[103] However, despite the IAT Report's recommendation for an intensive program of interdisciplinary recruitment aimed at balancing the skills mix and representation of women, francophones and minorities in the Service,[104] the recruitment was still biased in favour of anglophone white males. Recruitment was also lacking in its balancing of skills. All new applicants had to have a university degree. However, the preferred degree was in political science, with the result that the skills mix advocated by the IAT Report was not achieved.

Discrimination showed itself in two ways. The first was the obligation imposed on all new recruits to submit to a polygraph test to be admitted into the Service. Ex-members of the RCMP Security Service were exempted from this test. SIRC opposed relentlessly – and apparently still does – the use of the polygraph on two grounds: its known unreliability (once more, recently acknowledged by the FBI)[105] and the use of the test to question applicants, not only about their loyalty to Canada and the agency, but also about their "lifestyle." The issue of lifestyle had an impact on the profile of

---

102 Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security under the Law*, *supra* note 58, vol. I at 95ff; see also Cléroux, *Official Secrets: The Story behind the Canadian Security Intelligence Service*, *supra* note 9 at 31ff.

103 SIRC *Annual Report 1989-90* at 9.

104 Independent Advisory Team on the Canadian Security Intelligence Service, *People and Process in Transition*, *supra* note 40 at 16.

105 U.S., National Research Council, *supra* note 3.

the candidates identified as having a high potential. Judging from those graduate students I knew to have applied to CSIS, the required profile was one of conformity, if not of conformism. The good candidate would perform well on all indicators, without showing characteristics that stood out. According to the latest information from SIRC and CSIS, lifestyle polygraph tests are no longer used.

I have already referred to the second ground of discrimination. The second-rate status afforded to civilian analysts within CSIS – and within all police forces – was denounced in the 1981 McDonald Commission report, yet endured in 1999.**In my opinion, the Commission should be concerned about whether this has been remedied. It is inconsistent to stress the importance of rigorous analysis and yet to discriminate against those who provide that analysis by limiting their career options. It is the best way to keep the best away.**

3.3 Training

Training is one of the most vital instruments for imparting a professional culture to members joining an organization. Unfortunately, it is difficult to speak in an informed manner about CSIS training, since very limited information is available through open sources about training. For instance, the CSIS web site says nothing on the topic.

However, the following is apparent. First, an uphill battle had to be fought to convince CSIS of the need to train its intelligence officers. The Stephenson Academy was closed in 1987. This battle was won and the academy reopened. CSIS recruits are now exposed to a training curriculum that extends over several years.

Second, CSIS had to divest itself of the militaristic training that all RCMP recruits had to undergo. This kind of drilling rested on the premise that disciplining the body was the first step to fostering the identification of the newcomer with the organization.[106] As far as I can see, this aspect of training was suppressed by CSIS. I gave a course on terrorism at the CSIS Academy. I enjoyed complete freedom about the content of my lectures, and there was nothing stilted in the atmosphere in the classes. The only feature different from my normal teaching environment was the presence of a seasoned CSIS agent at the lectures. The agent joined freely in the discussion. I found this to be a positive aspect of the training.

---

106 Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security under the Law*, *supra* note 58, vol. II at 708.

Needless to say, **the Commission should, in my view, exercise its powers of investigation and go deeper into this crucial issue of training.**

3.4 Internationalization

I previously referred to CSIS setting up the Transnational Criminal Activities Unit in 1995-96. This occurred within the framework of an increasing number of international initiatives on several fronts. CSIS was created in 1984 as a domestic security intelligence agency without regard for the fact that most Western democracies with a domestic intelligence agency also had a foreign intelligence agency. In the present context of globalization, the line separating domestic and foreign intelligence is blurred, and the protection of national security requires both types of intelligence. SIRC had criticized CSIS quite early in its history saying that, "It seemed to us that information supplied by friendly foreign intelligence services might too easily be accepted by CSIS at face value."[107] CSIS responded by increasing the number of its international arrangements. As of March 1996, the Service had a total of 202 arrangements with 123 countries and three international organizations. CSIS declared that, "[M]any of our security intelligence threats originate overseas . . . . Given the diversity of the changes in the global security environment, a major challenge for the Service is to help prevent these conflicts from becoming Canadian domestic security problems."[108] To achieve this goal of prevention, CSIS increased the number of Security Liaison Officers posted to foreign countries, despite the difficult working conditions they faced abroad.[109] As permitted by section 16 of the *Canadian Security Intelligence Service Act* (*CSIS Act*), CSIS is now collecting foreign intelligence for the Minister of Foreign Affairs and for the Minister of National Defence.[110] The RCMP also operates at the international level in transnational investigations and by assisting in the training of police forces in developing countries. However, the international vocation of the RCMP is not as explicit and potentially wide-ranging as that of CSIS.

Internationalization has obvious implications for the occupational and organizational culture of an agency. First, as I have stressed, the custom in Western democracies is to have two separate security intelligence agencies, one operating within the country and another operating

---

107 SIRC *Annual Report 1986-87* at 23.
108 Canadian Security Intelligence Service, *1997 Public Report*, Part I.
109 SIRC *Annual Report 2000-2001* at 5-6.
110 *Ibid.* at 26ff; SIRC *Annual Report* 2001-2002 at 76ff.

abroad. If the present trend persists, CSIS may become *de facto* a security intelligence agency qualifying as **both a domestic and a foreign-oriented agency**. The professional culture of such an agency is bound to differ from the current culture of CSIS. If for all practical purposes CSIS becomes a domestic/foreign security intelligence agency, it will harbour three layers of professional culture: (1) the remnant of a police culture (for example, one that still discriminates between officers of the Service and "civilian analysts"); (2) the dominant domestic security intelligence culture and the attendant frictions with law enforcement agencies; and (3) the imported foreign intelligence culture. This multi-layering of various professional cultures may disorient the members of the Service. Second, and on a more positive note, it is to be expected that the Service's growing international commitment will further loosen the "in-group/out-group" dichotomy. Finally, the difference between Canada and its partners must not be obliterated to the point that the Canadian national interest would be conflated with the interests of Canada's friendly partners. Some twenty years ago, SIRC issued the following warning to CSIS: "[W]e sensed that CSIS might be too quick to accept the foreign policy underpinnings of this information [provided by friendly foreign intelligence services] instead of recasting it in terms of Canadian policy . . . ."[111] This warning remains relevant today, particularly in the light of the O'Connor report on the Maher Arar affair.

3.5 Human Rights

Developing and reinforcing a culture favourable to respecting human rights is particularly acute when it comes to cooperating with foreign agencies. CSIS was created to get rid of the RCMP Security Service culture of "institutionalized wrongdoing" that the McDonald Commission found to be prevalent. An array of mechanisms – a lessening of legal powers, judicial control, ministerial and sub-ministerial directives, an Inspector General, a review committee – was put in place to prevent CSIS from drifting into the same organizational territory as the former RCMP Security Service. Despite individual complaints (particularly about security clearance and immigration screening) and some unwelcome incidents, these mechanisms have worked on the whole, and it cannot be claimed that CSIS has become a clone of the RCMP Security Service in its approach to the human rights of Canadians and others living in Canada.

---

111 SIRC *Annual Report 1986-87* at 23.

The internationalization of the activities of CSIS called for a new vigilance. Although one would wish for an ideal world where the Service's foreign contacts would all have satisfactory human rights records, the reality is that many do not, and CSIS still has to deal with them to fulfill its duties.[112] SIRC revisited this issue in several of its subsequent reports. At the turn of the millennium, its statement of caution about protecting human rights had a prophetic undertone it light of future events: "*We believe the Service should take all possible care to ensure that the information it provides is not used to assist in the violation of human rights.* To that end, SLOs [Security Liaison Officers] are obligated to give the rest of the Service timely and accurate assessments of an agency's human rights record and of its propensity to pass information on to third parties without authorization."[113] In light of the findings of the O'Connor inquiry, it seems that CSIS heeded this advice, but that the RCMP did not. In its volume containing analysis and recommendations, the O'Connor report states that CSIS has a counterterrorist unit staffed by highly specialized analysts with eminent training. It further argues that the members of the RCMP involved in "Project A-O Canada," which led to the sharing with U.S. counter-terrorist agents of information that was both detrimental to Mr. Maher Arar and inaccurate, did not have the competence to pursue counter-terrorist investigations and viewed the Arar investigation as just one criminal investigation among many others. The O'Connor report also notes that the police involved in Project A-O Canada could have relied on CSIS or on the competence of the RCMP national security unit operating from the Ottawa Headquarters, but did not.[114]

The parts cited from the 2006 O'Connor report touch on at least five issues that I have discussed: (1) the criminal investigation culture versus the security intelligence culture; (2) the poor level of cooperation between units of the RCMP and CSIS; (3) the contrasting attitudes of agents from both agencies, depending on whether they are at headquarters or operating in the regions; (4) the cautiousness to be exercised in dealing with foreign agencies, even friendly ones; (5) relics of the RCMP Security Service high-handedness towards human rights. On some of these issues, it appears that little progress was made since the birth of CSIS in July 1984. More important, these concerns also raise the spectre of the questionable

---

112 SIRC *Annual Report 1998-99* at 28.

113 SIRC *Annual Report 2000-01* at 7 [emphasis added].

114 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar, supra* note 54, Vol. III, chapter 3, section 2.4.

ability of local RCMP investigators to conduct an investigation into a terrorist incident.

3.6 Accountability

CSIS and the RCMP differ in their accountability structures. The main difference lies in external review. The RCMP is accountable in this respect to two bodies. The Commission for Public Complaints against the RCMP (CPC) handles complaints from the public. The RCMP External Review Committee (ERC) has the mandate for civilian oversight of labour relations within the Force, and reviews grievances as well as appeals regarding formal disciplinary measures. The operations of CSIS are externally reviewed by SIRC. The overwhelming difference between SIRC and the RCMP's CPC and ERC is that SIRC, unlike its RCMP counterparts, is not limited to examining individual complaints. The CPC and the ERC play almost no role in defining RCMP policies. In contrast, SIRC reviews the operations of CSIS and, most significantly, makes recommendations that have an impact on the structure of the Service (for example, leading to the dismantling of the Counter-Subversion Branch) and its policies (for example, training). During the early years of CSIS, SIRC played a decisive role in steering it away from the culture of institutional wrongdoing that prevailed within the RCMP Security Service, and in shaping its occupational and organizational culture. Indeed, it is my conviction that SIRC was a strong component of this culture in the early years of the Service. It may be that the influence of SIRC on CSIS has somewhat decreased over the years.

In media interviews given to the CBC in 2006, the former chair of the CPC, Shirley Heafy, bitterly denounced the lack of cooperation from the RCMP during her tenure. In its second report, the O'Connor Commission proposed that the RCMP accountability mechanisms in the field of national security be completely restructured to ensure that a new body had SIRC-like audit and investigation powers and was not limited to the hearing of complaints.[115] On 14 December, 2007. the Task Force on Governance and Culture Change in the RCMP, presided by Mr. David Brown, recommended in its report that an independent complaint commission with increased powers be established for the RCMP.

---

115 Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Minister of Public Works and Government Services, 2006) (Chair: Dennis O'Connor).

SIRC generally enjoyed much greater cooperation from CSIS. However, in a declassified June 7, 2005, ruling by SIRC on the complaint by Bhupinder S. Liddar against CSIS and the Deputy Head of the Department of Foreign Affairs and International Trade, the then chair of SIRC, the Hon. Paule Gauthier, concluded that SIRC was "purposefully misled by the Service in this incident…."[116] Further, she stated, "In any case, I conclude that the Service provided me with misleading answers to my questions in order to prevent Mr. Liddar or the Review Committee from having information – that would have been known by the Service to be potentially relevant to my investigation – brought to our attention."[117] This indictment is all the more significant in light of the length of Ms. Gauthier's tenure on SIRC. She is the only person to have been a member of SIRC from its creation in 1984 until 2005, when she was replaced by the Hon. Gary Filmon.

4. PROFESSIONAL CULTURES IN CONTRAST AND IN CONTACT

I will now bring together the conclusions of the previous discussions in two tables. These tables summarize the contrasting features of CSIS and the RCMP that were discussed above. They also add to them – in particular Table 2, which presents new material in relation to the public **symbolic resonance** of the RCMP and law enforcement forces on the one hand, and of CSIS and security intelligence agencies on the other. With respect to certain features, the contrast is marked, as it is in respect to the evidence versus intelligence conundrum. In other cases – for instance, internationalization – the contrast is less pronounced, as both agencies operate in part on the international level (this part being nonetheless greater for CSIS). Table 1 presents the elements and determinants of the RCMP and CSIS occupational and organizational cultures. For example, the degree of centralization of an agency is an organizational fact. However, the regional autonomy that flows from decentralization belongs to the professional culture.

---

116 Full cite needed?Para 8.
117 Ibid at Para 10.

Table 1
Elements and determinants of occupational and organizational culture

POLICE - RCMP	**SECURITY INTELLIGENCE - CSIS**
1. REACTIVE - after the fact	1. PREVENTIVE/PROACTIVE - before the fact
2. *Mobilized by CITIZEN COMPLAINANTS*	2. *SELF TRIGGERING - mobilized by Government*
3. Collect EVIDENCE for public proceedings	3. Collect secret INTELLIGENCE to advise government
4. Powers of *COERCION*	4. *Powers of INTRUSION*
5. Institutional clients: CROWN and JUDICIARY	5. Institutional clients: branches of the EXECUTIVE
6. Bound by rules of legal PROCEDURE	6. Fewer rules and more DISCRETIONARY POWER
7. *Protected from external (political) INTERFERENCE – INDEPENDENT body*	7. Subject to MINISTERIAL WRITTEN DIRECTIONS
8. HIGH PUBLIC PROFILE and openness	8. LOW PUBLIC PROFILE: SECRECY and stealth
9. CASE-BY-CASE ACCOUNTABILITY driven by individual complaints	9. Organizational, SYSTEMIC and individual complaint ACCOUNTABILITY
10. High internal TERRITORIALIZATION – low international involvement	10. Centered on domestic operations with increasing trend towards INTERNATIONALIZATION
11. DECENTRALIZED organizational structure	11. CENTRALIZED organizational structure
12. HIGH REGIONAL AUTONOMY	12. LOW REGIONAL AUTONOMY
13. MILITARISTIC structure and training	13. CIVILIAN organization with ACADEMIC training

As Table I shows, some of these features form a sequence, such as features 2 to 6 on the left, as they relate to the police. The police are mobilized by a complainant (often one calling the emergency 911 number). When there is enough are indication that a crime has been committed, police

investigators collect evidence and when it is sufficiently strong, they use their powers of coercion to perform an arrest. The person arrested is charged and brought to trial. The trial is conducted according to compulsory rules of procedure and exacting standards of proof.

Three other attributes distinguish police agencies from security intelligence agencies. These attributes were not discussed in this paper as explicitly as those mentioned above.

The first is the issue of mobilization. Police intervention is in the great majority of cases triggered by an external complainant, generally a citizen. In contrast, intelligence agents scan the social environment on their own, looking for security threats, or they follow written directives issued by a government minister. Their targeting is most often triggered from inside the agency.

The second distinction concerns means. In both the law and research literature, the police are defined by their use of **legitimate force**. Security intelligence agents are characterized by their use of powers of **covert intrusion** to collect concealed information.

The third distinction relates to independence. The police operate at arm's length from the executive branch of government, with the RCMP jealously defending its independence from political interference. In contrast, CSIS is explicitly bound by law to the executive branch.[118] It is interesting to note in this respect that the RCMP Security Service had no enabling law, its existence resting on executive orders. This was also the situation with CSE for more than half a century.

As these words are used in the literature, occupational and organizational culture refer to the internal professional culture of an agency, *as it springs from the in-group*. Symbolic features, as I use the words, refer both to the socio-psychological impact of an agency on the outside world and the external characteristics that are attributed to the agency and its members. These characteristics attributed from the outside have a feed-back action, looping back into the internal professional culture and shaping it to a significant extent.

---

118 *Canadian Security Intelligence Service Act*, *supra* note 39, sections 6(2), 12-16.

Table 2
Symbolic features

POLICE – RCMP	SECURITY INTELLIGENCE – CSIS
1. Canadian icon	1. Canadian exemplar
2. Symbol of the law	2. Symbol of the power of the State
3. Law-abidingness	3. Extra-legality
4. Trust	4. Fear

I will briefly comment on these features, some of which are self-evident. (1) The "Mounties," along with the maple leaf and the beaver, are a symbol of Canada and have generated a rich hagiography ("They always get their man."). Their iconic character is one of the most deeply embedded aspects of their culture. They are also world symbols of police integrity. The symbolic resonance of CSIS is not on a par with that of the RCMP. Nevertheless, the accountability structure of CSIS and its commitment to human rights is often cited at the international level. (2) The police are the most potent symbol of the law (indeed, they are commonly referred to as "the law"). Security intelligence services, also designated as the "political police," symbolize the power of the State. In this respect, their symbolic functioning is very different from that of the police. The police are *visible* symbols of the law, whereas the intelligence services are *stealthy* symbols thriving on rumours and innuendo. (3) This third contrast is easy to misunderstand. The drive to separate the Security Service from the RCMP was initially started by the Mackenzie Commission report.[119] The main reason for Commissioner Mackenzie's recommendation to separate the Security Service from the RCMP was his belief that it was "unavoidable" that a security service would be involved in operations that would contradict the spirit, if not the letter, of the law, and that it would take part in covert activities that would violate civil rights. As representatives of the law, the police could not afford to be involved in such contradictory behaviour.[120] However, the research literature on the police stresses that policing is a "tainted" occupation[121] and that the police are in fact performing "dirty work." This apparent contradiction disappears to a great extent when we distinguish between reality and symbol. Despite the fact that the police may **in fact** often break the law, it is not admissible to grant **legitimacy** to these violations **on the levels of principle and value**, where appearances must be maintained.

---

119 Royal Commission on Security, *Abridged Report of the Royal Commission on Security*, *supra* note 65.
120 *Ibid.* at para. 57.
121 Egon Bittner *Aspects of Police Work* (Boston: Northeastern University Press, 1972) at 95-96.

The situation is quite different for intelligence services. Their lawlessness is the stuff of their legend. Their abuses are either legalized or covertly authorized by the executive. Appearances are completely reversed in the case of intelligence services. The rogue culture fostered by fiction and by the media is that an intelligence agency is efficient in proportion to its lack of respect for all rules, whereas these services are in fact closely monitored and more strictly bound by the legal rule and internal regulations than is believed. (4) Manning[122] and others have stressed that policing relied on trust. Simply put, you have to trust the police in order to call them. All reforms of policing that followed World War II – team policing, community policing, "*police de proximité*" – were predicated upon the establishment of trust between the police and the public. In contrast, the action of security services more often elicit fear than trust, even in democracies, where too much political policing is said to have a "chilling effect." Paradoxically, the attitudes of these agencies towards their covert informants seem to follow reverse logic. Police informants are generally handled by alternating the carrot and the stick – fear of the stick playing the dominant role. In contrast, intelligence agents appear to be fiercely loyal to their sources, to the point of circumventing the law to protect their identity.

5. TO CONCLUDE

The preceding section has been in part devoted to a synthesis of the paper. There is no need to go over the same ground again here. I will conclude by asking two questions:

(1) What went wrong in the Air India investigation and subsequent 2003 trial, which ended in the acquittal of the accused in 2005?

(2) What needs to be done?

My answers to both questions are tentative and meant as suggestions for future inquiries.

5.1 What went wrong?

I have done first-hand research from police archives (1990-2002) on the criminal investigation of homicides (all kinds). In the course of this research, I also reviewed the research literature on this topic. The main

---

122 P.K. Manning, *Policing Contingencies* (Chicago: The University of Chicago Press, 2003).

finding of my research, which is confirmed by all other research, is that a high proportion of homicide cases – 71 per cent of the 153 cases my research examined – are solved within 24 hours, and 83 per cent are solved in less than a week.[123] The longer an investigation extends, the less likely it is that the crime will be solved. In light of this highly corroborated finding, the first months that followed the June 1985 Air India bombings were of crucial importance. Was the failure to solve the case when it could have been solved (according to the probability of clearing a case) due to a clash of professional cultures between the RCMP conducting the investigation and CSIS? As I suggested earlier, my hypothesis is not only that we should answer this question in the negative, but that we should resist its handy simplicity. CSIS had been created only eleven months before the tragedy and was essentially staffed by ex-RCMP Security Service members who had not yet developed an intelligence culture. This is overwhelming clear from SIRC's annual reports from 1984-85 to 1989-1990. What happened in British Columbia after the Air India bombings much more closely resembles an institutional police panic and improvisation, and investigative incompetence, than anything else.

This last observation goes beyond a purely factual explanation as it involves a value judgment on the quality of the work performed by the investigators. I would add to this my view that RCMP and CSIS estrangement from the Indo-Canadian community also played a great part in the failure to solve the case. The agencies had few contacts within this community and probably had little idea of where to start.

Finally, after all these years, the Crown's case in the 2003 criminal proceedings rested on the testimony of two informants, one of them a typical police informant and the other a witness who was emotionally involved with one of the accused and who agreed to come forward. Neither of the informants convinced Judge Josephson. His 2005 verdict was not appealed.

5.2 What needs to be done?

The answer to this question will no doubt take the form of many recommendations. This paper is limited in scope. I will therefore limit myself to making two suggestions.

---

123 Jean-Paul Brodeur "L'enquete policiere' in Criminologie (Montreal: Les Presses de l'Universities de Montreal, 2005); Charles Wellford and James Cronin, *An Analysis of the Variables Affecting the Clearance of Homicides: A Multistate Study* (Washington, DC: Justice Research and Statistics Association, 1999). (Brodeur, 2005;

5.2.1 Joint targeting with separate means

First, evidence and intelligence collide in two situations:

(1) when the evidence and the intelligence coincide through the potential testimony of a single individual (the worst case scenario). In the proceedings against Khela and Dhillon, the testimony of a source ("Billy Joe"), whose identity the counter-terrorism police wanted to keep secret, was the sole foundation of the prosecution's case. Billy Joe's identity was ultimately protected and both accused were acquitted; or

(2) when they are produced by the same physical means, whether as intelligence or as criminal evidence.. An example is the erasure by CSIS of the audio-tapes that might also have been crucial evidence for the police during the first year of the Air India investigations. One way out of this predicament would be *joint targeting.* **If CSIS had solid intelligence on the clear and present threat presented by an individual or group, it could pass this information to a law enforcement agency so that the agency might target the same individual or group for its own evidentiary purposes, using its own, separate, means, instead of using the intelligence collected by CSIS for purposes of threat assessment.** This arrangement could be implemented through the senior level committee contemplated under the September 29, 2006, MOU between the RCMP and CSIS. The general goal of this committee is to coordinate the investigations of both agencies.[124]

5.2.2 Revisiting *Stinchcombe*

Although I have no academic legal training, I will venture to trespass on guarded territory in offering my assessment that the *Stinchcombe* ruling has now been diverted from its original purpose. That original purpose was not only to preserve the rights of the defendant but to facilitate and speed up court proceedings. It has in the latter regard had the opposite effect. As already mentioned, the preliminary hearing of the four teens accused of involvement in an alleged 2006 Toronto bomb plot required the disclosure of two million pages of evidence. It seems to me that

---

[124] RCMP/CSIS MOU 2006 at (Part 1, section 3).

this situation is not propitious for justice. My suggestion is to clarify the disclosure requirements in Canadian criminal proceedings through ministerial guidelines or new legislation.

REFERENCES

Amnesty International, *United Kingdom: Northern Ireland: killings by security forces and "supergrass" trials* (London (UK): Amnesty International, 1988).

Christopher Andrew, *Her Majesty's Secret Service* (New York: Viking Press, 1986).

Christopher Andrew and Oleg Gordievsky, *KGB - The Inside Story* (London: Hodder & Stoughton, 1990).

Kim Bolan, *Loss of Faith: How the Air India Bombers Got Away with Murder* (Toronto: McClelland & Stewart, 2005).

Jean-Paul Brodeur, "*L'enquête policière*" in *Criminologie* (Montréal: Les Presses de l'Université de Montréal, 2005) 39.

Jean-Paul Brodeur, "Cops and spooks: the uneasy partnership" in Tim Newburn, ed., *Policing: Key Readings* (Cullompton (Devon, UK): Willan Publishing, 2005).

Jean-Paul Brodeur, "Undercover Policing in Canada: A Study of its Consequences" in C. Fijnaut and G.T. Marx, eds., *Police Surveillance in Comparative Perspective* (The Hague: Kluwer Law International, 1995).

Jean-Paul Brodeur, "La Gendarmerie Royale du Canada," *Les Cahiers de la Sécurité intérieure, Gendarmeries et polices à statut militaire*, (Paris: Institut des Hautes Études de la Sécurité intérieure, La Documentation française, 1992) 173.

Jean-Paul Brodeur, "High and Low Policing: Remarks About the Policing of Political Activities" (1983) 30 Social Problems 507, reprinted in R. Reiner, ed., *Police Discretion and Accountability: Policing Vol. II* (Aldershot (UK): Dartmouth Pub., 1996) 261.

Jean-Paul Brodeur, "Legitimizing Police Deviance" in Clifford Shearing, ed., *Organizational Police Deviance* (Toronto: Butterworths, 1981) 127.

Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar* (3 vols.) (Ottawa: Minister of Public Works and Government Services, 2006) (Chair: Dennis O'Connor).

Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Minister of Public Works and Government Services, 2006) (Chair: Dennis O'Connor).

Canada, House of Commons, *In Flux but not in Crisis: Report of the Special Committee on the Review of the CSIS Act and the Security Offences Act* (Ottawa: Supply and Services Canada, 1990).

Canada, Senate, *Terrorism: Report of the Second Special Committee of the Senate on Terrorism and Public Safety* (Ottawa: Minister of Supply and Services, 1989).

Canada, Senate, *Terrorism: Report of the Senate Special Committee on Terrorism and Public Safety* (Ottawa: Minister of Supply and Services Canada, 1987).

Canada, Senate, *A Delicate Balance: A Security Intelligence Service in a Democratic Society: Report of the Special Committee of the Senate on the Canadian Security Intelligence Service* (Ottawa: Supply and Services Canada, 1983).

Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report: Freedom and Security under the Law*, 2 vols. (Ottawa: Minister of Supply and Services Canada, 1981) ("McDonald Commission," Chair: David C. McDonald).

Canada, Royal Commission on Security, *Abridged Report of the Royal Commission on Security* (Ottawa: Queen's Printer, 1969) (the "Mackenzie Commission").

Canadian Security Intelligence Service, *Annual Reports* (Ottawa, 1992-2006).

Richard Cléroux, *Official Secrets: The Story behind the Canadian Security Intelligence Service* (Toronto: McGraw-Hill Ryerson, 1990).

William Colby, *Honorable Men: My Life in the CIA* (New York: Simon and Schuster, 1978).
Alain Dewerpe, *Espion: Une Anthropologie historique du secret d'État contemporain* (Paris: Gallimard, 1994).

Allen W. Dulles, *The Craft of Intelligence* (New York: Signet Books, 1965).
Richard V. Ericson and Kevin T. Haggerty *Policing the Risk Society* (Toronto: University of Toronto Press, 1997).
Janet Foster, "Police cultures" in Tim Newburn, ed., *Handbook of Policing* (Cullompton (Devon; UK), 2003) 196.

Mike Frost and Michel Gratton, *Spyworld* (Toronto: Doubleday, 1994).

Tony Gifford, *Supergrasses: the use of accomplice evidence in Northern Ireland* (London: Cobden Trust, 1984).

Steven Greer, *Supergrasses: A Study in Anti-Terrorist Law Enforcement in Northern Ireland* (Oxford: Oxford University Press, 1995).

Tom Mangold, *Cold Warrior: James Jesus Angleton: The CIA's Master Spy Hunter* (London: Simon and Schuster, 1991).

Peter Kirby. Manning, *Policing Contingencies* (Chicago: The University of Chicago Press, 2003).

Victor Marchetti and John D. Marks, *The CIA and the Cult of Intelligence* (New York: Alfred A. Knopf, 1974).

David C. Martin, *Wilderness of Mirrors* (New York: Harper and Row, 1980).
Andrew Mitrovica, *Covert Entry: Spies, Lies and Crimes Inside Canada's Secret Service* (Toronto: Random House, 2002).

Andrew Mitrovica and Jeff Sallot, "CSIS agent destroyed Air-India evidence," *The Globe and Mail* (January 26, 2000) A1-A2.

U.S., National Research Council, National Research Committee to Review Research on Police Policy and Practices, Committee on Law and Justice, Division of Behavioral and Social Sciences and Education, Westley Skogan and Kathleen Frydl, eds., *Fairness and Effectiveness in Policing: The Evidence* (Washington, DC: The National Academies Press, 2003).

U.S., National Research Council, Committee to Review the Scientific Evidence on the Polygraph, Board on Behavioral, Cognitive, and Sensory Sciences and Committee on National Statistics, Division of Behavioral and Social Sciences and Education, *The Polygraph and Lie Detection* (Washington, DC: The National Academies Press, 2003).

Andre Normandeau and Barry Leighton, *A Vision of the Future of Policing in Canada: Police-Challenge 2000: Background Document* (Ottawa: Police and Security Branch, Ministry of the Solicitor General, 1990).

Thomas Powers, *The Man Who Kept the Secrets: Richard Helms and the CIA* (New York: Alfred A. Knopf, 1979).

Québec, *Rapport de la Commission sur des Opérations Policières en Territoire Québécois* (the Keable Report) (Québec: Ministère des Communications, 1981).

The *Honourable Bob Rae, Lessons to Be Learned,* the report of the Honourable Bob Rae, Independent Advisor to the Minister of Public Safety and Emergency Preparedness, on outstanding questions with respect to the bombing of Air India Flight 182 (Ottawa: Air India Review Secretariat, 2005)

Andrew Sanders, "From Suspect to Trial" in M. Maguire, R. Morgan and R. Reiner, eds.,) *The Oxford Handbook of Criminology* (Oxford: Oxford University Press, 1994) 773.
John Sawatsky, *For Services Rendered: Leslie James Bennett and the RCMP Security Service* (Toronto: Doubleday, 1982).

Security Intelligence Review Committee, *Annual Reports* (1984-85 to 2005-06) (Ottawa: Minister of Supply and Services).

Security Intelligence Review Committee, *The Heritage Front Affair: Report to the Solicitor General of Canada* (Ottawa: Security Intelligence Review Committee, 1994).

Security Intelligence Review Committee, *Closing the Gaps: Official Languages and Staff Relations in the Canadian Security Intelligence Service* (Ottawa: Minister of Supply and Services Canada, 1987).

Independent Advisory Team on the Canadian Security Intelligence Service, *People and Process in Transition* (report to the Solicitor General) (Ottawa: Ministry of Supply and Services Canada, 1987).

U.S., Senate Select Committee on Intelligence, "September 11 and the Imperative of Reform in the U.S. Intelligence Community: Additional Views of Senator Richard C. Shelby, Vice Chairman, Senate Select Committee on Intelligence" (Washington, DC: Congress, 2002) http://intelligence.senate.gov/shelby.pdf

P.A.J. Waddington, "Police (canteen) sub-culture: an appreciation" in Tim Newburn, ed., *Policing: Key Readings* (Cullompton (Devon, UK): Willan Publishing, 2005) 364.

Charles Wellford and James Cronin, *An Analysis of the Variables Affecting the Clearance of Homicides: A Multistate Study* (Washington, DC: Justice Research and Statistics Association, 1999).

Giuliano Zaccardelli, Speaking notes for a presentation on intelligence-led policing at the Canadian Association of Chiefs of Police Conference, Ottawa, Ontario, August 23, 2005.

Jean-Paul Brodeur holds a Ph.D. in philosophy from the *Université de Paris* and a Masters in criminology from the *Université de Montréal* (UdeM). He also studied Sanskrit at the *École pratique des Hautes Études* and the *École des langues orientales* in Paris. He has taught philosophy at the *Université du Québec à Montréal* and is presently a full professor at the *École de criminologie* (UdeM). He is also the current director of the Centre international de criminologie comparée/ International Centre for Comparative Criminologie at the UdeM. He is a former president of the Canadian Association for the Study of Intelligence and Security (CASIS). He was awarded a Killam scholarship (2003/2004) and was an invited fellow at the *Institut des Hautes Études de la Sécurité Intérieure* in Paris and at the Institute of Criminology of Cambridge University (UK). Professor Brodeur has been a member of the Royal Society of Canada since 1989.

He was part of more than 20 commissions of inquiry and government task forces, both at the federal and the provincial Québec levels. He was research director for the *Commission d'enquête sur des opérations policières en territoire québécois* (Keable Commission, 1978-1980), which conducted in Québec an investigation into counterterrorism that was parallel to the McDonald inquiry at the federal level. Both inquiries assessed whether the counterterrorist tactics of the Royal Canadian Mounted Police (RCMP) and other police forces in Québec were law-abiding and respectful of human rights. He also assisted Counsel Jean-François Duchaîne in his investigation of the 1970 October Crisis. After the creation of the Canadian Security Intelligence Service in 1984, he was a consultant for the Security Intelligence Review Committee (SIRC). He was also a member of Public Complaints Review Committee of the *Sûreté du Québec* (1989-1993) and conducted a study on the use of police informants for the Commission for Public Complaints against the RCMP (1996). During the years 1984-1987, he was research director for the Canadian Sentencing Commission.

Professor Brodeur was part of the research staff of the inquiry into the deployment of Canadian Forces in Somalia (the Létourneau Inquiry - 1995-1997). His study was published under the title *Violence and Racial Prejudice in the Context of Peacekeeping Operations/Violence et préjugé raciaux dans les missions de maintien de la paix* (Ottawa, 1997). He was a consultant for the Law reform Commission of Canada, for which he conducted a study on visible minorities and Canadian justice (1991), and for the Law Commission of Canada, which published his study on the nature of crime (2003).

Jean-Paul Brodeur has published 18 books and more than 160 articles on policing, criminal justice and politically motivated deviance. He was asked by the *Encyclopedia Britannica* to update its articles on *Police* and *Police technology* for its current edition. His latest books are *Democracy, Law and Security* (2003, with Peter Gill and Dennis Töllborg) and *Citoyens et Délateurs* (with Fabien Jobard). He is now completing a *Treatise on Policing* (September 2008).

Commission of Inquiry
into the Investigation
of the Bombing of
Air India Flight 182